

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN2010/078611

International filing date: 10 November 2010 (10.11.2010)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 201010102646.2
Filing date: 25 January 2010 (25.01.2010)

Date of receipt at the International Bureau: 04 March 2011 (04.03.2011)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

Charter Communications, Inc. - Exhibit 1002
Charter Communications, Inc. v. Iarnach
Technologies, Ltd.

证 明

本证明之附件是向本局提交的下列专利申请文件副本。

申 请 日： 2010. 01. 25

申 请 号： 201010102646. 2

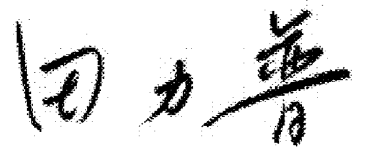
申 请 类 别： 发明专利

发 明 创 造 名 称： 一种无源光网络系统组播业务加密方法和装置

申 请 人： 中兴通讯股份有限公司

发明人或设计人： 张德智、袁立权

中华人民共和国
国家知识产权局局长



2011年02月16日

1、 一种无源光网络系统组播业务加密方法，包括

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

2、 如权利要求 1 所述的方法，其特征在于，

所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

3、 如权利要求 1 或 2 所述的方法，其特征在于，

所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

4、 如权利要求 1 所述的方法，其特征在于，

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

5、 如权利要求 1 所述的方法，其特征在于，

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

6、 如权利要求 1 或 2 所述的方法，其特征在于，

所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

5 7、 一种无源光网络系统组播业务加密装置，包括密钥生成单元，加密单元，发送单元，其中：

所述密钥生成单元，用于生成公共密钥；

所述加密单元，用于对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

10 所述发送单元，用于发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

8、 如权利要求 7 所述的装置，其特征在于，

15 所述装置还包括老化时间设置单元，用于为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

9、 如权利要求 7 所述的装置，其特征在于，

20 所述发送单元，进一步用于判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，用于在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

10、 如权利要求 7 或 9 所述的装置，其特征在于，

25 所述发送单元在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

一种无源光网络系统组播业务加密方法和装置

5 技术领域

本发明涉及光通信领域，具体涉及一种用于 PON（Passive Optical Network，无源光网络）系统中对组播业务数据进行加密的方法和装置。

背景技术

10 无源光网络的结构，是一个 PON 口对应于多个 PON 终端用户 ONU（Optical Network Unit，光网络单元）设备，且在下行链路上，局侧 OLT（Optical Line Terminal，光线路终端）发出的所有数据，每个用户 ONU 都能够进行接收。这里所说的“每个用户 ONU”包含合法用户和恶意用户两种情况：

15 拥有合法的注册信息，在物理连接到 PON 的某一根分支光纤后，可以和 OLT 交互消息进行注册，这种用户称之为合法用户；

不具有合法的注册信息，仅仅是在物理上连接到 PON 的某一根分支光纤，从不理会 OLT 发出的注册要求，仅接收下行信息，这种用户可以称之为恶意用户。

20 即使是合法用户，在其物理链接到一根分支光纤后，并在成功注册之前，也可以接收到 OLT PON 端口下发的各种明文数据包。目前 PON 技术中定义了一些加密机制，如 GPON（Gigabit-Capable Passive Optical Network，吉比特无源光网络）系统的 AES（Advanced Encryption Standard，高级加密标准）加密机制，或者 EPON（Ethernet Passive Optical Network，以太网无源光网络）
25 系统中的搅动加密机制和三重搅动加密机制等等，都是单播加密机制。对于组播数据（即 OLT PON 端口仅有一份业务数据下发，所有的用户或者符合要求的一部分用户接收、使用该业务数据），目前还没有有效的加密机制进行。一般运营商都是针对业务设置一个全网范围通用的密钥进行加密，但这

种机制的缺点是一旦密钥被恶意用户得知，其全网所有业务内容都将被解密窃取。

运营商在无源光网络 PON 中目前采用的方法是将组播业务数据包复制到每一个 PON 端口和用户 ONU 的单播通道上，应用单播机制进行加密，来
5 保护组播业务数据包不被恶意用户窃取。但是这种方法需要为每个 ONU 发送密钥，加重了 OLT 的负担。

发明内容

本发明要解决的技术问题是提供一种无源光网络系统组播业务加密方
10 法和装置，提高安全性，简化 OLT 加密机制的复杂性，减轻 OLT 负荷。

为解决上述技术问题，本发明提供了一种无源光网络系统组播业务加密方法，包括：

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公
15 共密钥加密；

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

进一步地，所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

进一步地，所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载
20 通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

进一步地，所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注
25 册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥, 所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据, 则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

进一步地, 不同承载通道上的组播业务数据使用的公共密钥相同或不同。

- 5 进一步地, 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时, 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

- 10 为解决上述技术问题, 本发明还提供了一种无源光网络系统组播业务加密装置, 包括密钥生成单元, 加密单元, 发送单元, 其中:

所述密钥生成单元, 用于生成公共密钥;

所述加密单元, 用于对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密;

- 15 所述发送单元, 用于发送加密后的组播业务数据, 以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元 (ONU)。

进一步地, 所述装置还包括老化时间设置单元, 用于为公共密钥设置老化时间, 当老化时间到达时, 通知所述密钥生成单元重新生成公共密钥。

- 20 进一步地, 所述发送单元, 进一步用于判断 ONU 注册成功且申请接收组播业务数据后, 主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU; 或者, 用于在接收到 ONU 请求密钥的请求后, 判断所述 ONU 注册成功且申请接收组播业务数据, 则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

- 25 进一步地, 所述发送单元在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时, 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制,可以将密码泄露后的影响范围从全网限制到某一个 PON 口,提高了组播业务内容的安全性。

5 另外,通过对无源光网络承载的组播业务数据进行加密后传输,以及仅将密钥发送给注册成功的用户,使得恶意用户无法获知上述密钥,且合法用户在注册之前也无法得到密钥,从而防止恶意用户窃取组播业务内容的非法行为,同时不会影响合法用户在注册后正常使用加密后的组播业务。

10 附图说明

此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

图 1 为本发明实施例一的流程图;

15 图 2 为本发明实施例二的流程图;

图 3 为本发明实施例三的流程图;

图 4 为本发明实施例四的流程图。

具体实施方式

20 本发明的发明构思是: OLT 生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的数据使用相同的公共密钥加密;所述 OLT 通过管理控制通道(例如 OMCI 或者 OAM)将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

25 ONU 获取公共密钥后,使用该密钥对承载通道上该 ONU 申请接收的组播业务数据进行解密。

优选地,OLT 定期维护该公钥,可以在生成公共密钥的同时为公共密钥

设置老化时间（如通过定时器设置），待老化时间到达后，重新生成公共密钥并使用新生成的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请接收所述组播业务数据的 ONU 发送新生成的公共密钥。多个公共密钥的老化时间可以相同也可以不同。或者 OLT 也可以在任何需要的时候，更新该公共密钥。

所述承载通道是 PON 的逻辑通道，可以是 GPON 端口承载的 GEM（通用封装格式，General Encapsulation Model）通道，或 EPON 端口的逻辑链路（Logical Link Identification, LLID）通道，且由 OLT 进行维护更新。

所述管理控制通道也是 PON 的逻辑通道，例如可以是 GPON 系统的 PLOAM 通道或 OMCI 通道，或者 EPON 系统中的扩展 OAM 通道。或者，采用数据通道发送公共密钥。

OLT 可同时生成多个公共密钥，分别用于对不同的承载通道进行数据加密。优选的，同一 PON 端口下的各条承载通道的公共密钥可以相同也可以不同，例如，可以设置每条承载通道有不同的公共密钥，也可以使部分承载通道使用相同的公共密钥。

当 OLT 对多条承载通道上的组播数据进行加密，且该多条承载通道可能发送给相同的 ONU 时，可在向 ONU 发送公共密钥的同时将使用该公共密钥进行组播业务数据加密的承载通道的承载通道标识一并发送给 ONU，即将承载所述组播业务数据的承载通道的承载通道标识发送给 ONU，以便 ONU 解密。但也不排除 ONU 通过逐一解密的方法找到使用该公共密钥的承载通道。

下面举例说明其实施方式，只要符合本专利的思想，采用其他实施方式也可以。下面就具体实时将来进行说明。

实施例一

本实施例为 GPON 系统传送公共密钥的实施例，应用范围是整个 GPON 物理端口，如图 1 所示，流程包括：

步骤 110，OLT 生成应用于组播业务的公共密钥；

步骤 120, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 130, ONU 上电, 接入 GPON 向 OLT 发起注册并申请组播业务;

关于具体的注册过程以及申请组播业务的过程, GPON 协议已经有相关定义, 本文不再赘述。

5 步骤 140, OLT 检测该 ONU 注册成功且申请组播业务, 将生成的公共密钥发送给该 ONU;

ONU 是否注册成功以及 ONU 申请何种组播业务在 OLT 上均有记录。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

10 OLT 可以采用 GPON 协议中的 PLOAM (Physical Layer Operation Administration Maintenance, 物理层操作管理维护) 通道, 或者 OMCI (ONU management and Control Interface, 光网络单元管理与控制接口) 通道或其他通道 (如数据通道) 将组播公共密钥传递给注册成功的 ONU。

15 步骤 150, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密。

实施例二

本实施例为 EPON 系统传送公共密钥且进行密钥更新的实施例, 应用范围是整个 EPON 物理端口, 如图 2 所示, 流程包括:

20 步骤 210, OLT 生成应用于组播业务的公共密钥, 并为该公共密钥设定一个定时器 T1;

该定时器用于控制公共密钥的老化时间。

步骤 220, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 230, ONU 上电, 接入 EPON 向 OLT 发起注册, 并申请组播业务;

25 具体的注册过程以及申请组播业务的过程, EPON 协议已经有相关定义, 本文不再赘述。

步骤 240, ONU 请求 OLT 发送组播业务公共密钥;

步骤 250, OLT 接收到 ONU 的请求后, 查询该 ONU 如果处于注册成功状态且该 ONU 申请组播业务, 则将生成的公共密钥发送给该 ONU;

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 260, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密;

步骤 270, 当 T1 定时器超时, OLT 重新生成新的公共密钥, 并重置 T1 定时器 (以便下次 T1 超时后再次更新密钥)。

当有其他 ONU 请求 OLT 发送组播业务公共密钥时, OLT 将新生成的公共密钥发送给请求公共密钥的 ONU。并且, OLT 还需要为已经发送过公共密钥的 ONU 更新公共密钥。

OLT 可以采用 EPON 系统中的管理控制通道 (如扩展 OAM 通道) 或数据通道将生成的组播公共密钥传递给注册成功的 ONU。

实施例三

本实施例为 GPON 系统中非法用户试图接入业务被拒绝的示例, 应用范围是整个 GPON 物理端口, 如图 3 所示, 流程包括:

步骤 310, OLT 生成应用于组播业务的公共密钥;

步骤 320, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 330, 恶意用户 ONU 接入 GPON;

恶意用户接入 GPON 后可能不发起注册, 但如果发起注册的话必定无法注册成功, 也无法申请组播业务。

步骤 340, 恶意用户 ONU 请求 OLT 发送组播业务公共密钥;

步骤 350, OLT 接收到请求后, 查询该 ONU 未能成功注册, 拒绝发送该组播公共密钥。

此时恶意 ONU 将无法获取组播公共密钥，也就无法对组播业务内容进行解密，运营商藉此防止了恶意用户的内容窃取。

实施例四

5 本实施例为 GPON 系统传送公共密钥的实施例，应用范围是 GPON 物理端口中对应某一组播业务的一个 GEM 通道，本实施例中的 ONU 仅申请了第一 GEM 通道上的组播业务，如图 4 所示，流程包括：

步骤 410，OLT 生成应用于第一 GEM 通道的组播公共密钥 A，以及应用于第二 GEM 通道的组播公共密钥 B；

10 步骤 420，OLT 将承载在第一 GEM 通道的组播业务数据用公共密钥 A 加密后传输，该通道所有 ONU 共享此公共密钥 A；

步骤 430，OLT 将承载在第二 GEM 通道的组播业务数据用公共密钥 B 加密后传输，该通道所有 ONU 共享此公共密钥 B；

上述步骤 420 和 430 的执行顺序不固定。

15 步骤 440，ONU 上电，接入 GPON 向 OLT 发起注册并申请组播业务；

步骤 450，OLT 检测到该 ONU 注册成功且申请接收的是第一 GEM 通道上的组播业务，将该公共密钥 A 和对应的第一 GEM 通道标识传送给该 ONU；

在其他实施例中，也可以由 ONU 主动发起密钥请求。

20 OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 460，ONU 接收到公共密钥 A 和对应的第一 GEM 通道标识后，对第一 GEM 通道中传输的组播业务数据进行解密。

ONU1 未接收到公钥 B，无法解密下行 GEM B 通道数据。可见，当同一 ONU 接收多个组播业务且该多个组播业务数据承载在不同的承载通道上时，
25 OLT 需要在发送公钥的同时将该公钥对应的承载通道标识发送给该 ONU。

OLT 可以采用 GPON 协议中的 PLOAM 通道维护通道，或者 OMCI 管

理通道或其他通道将组播公共密钥传递给注册成功的 ONU。

一个公共密钥可以用于一条 GEM 通道，也可以用于多条，即多条 GEM 通道共用一个密钥。

5 实现上述方法的 OLT 包括密钥生成单元，加密单元，发送单元，其中：
所述密钥生成单元，用于生成公共密钥；

所述加密单元，用于对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

10 所述发送单元，用于发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

优选地，所述装置还包括老化时间设置单元，用于对密钥生成单元生成的公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

15 所述发送单元在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

20 所述发送单元，进一步用于判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，用于在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

25 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

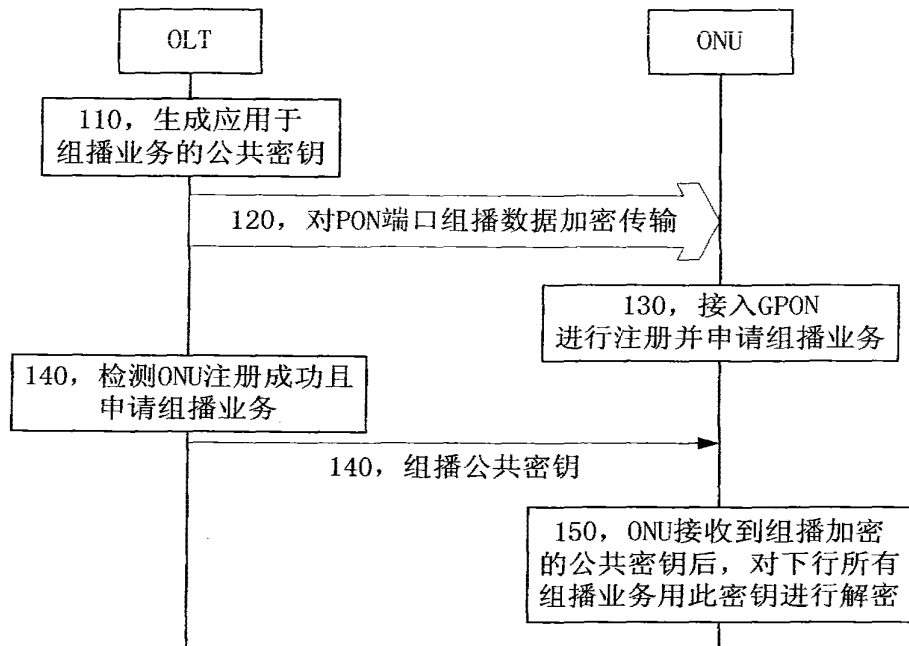


图 1

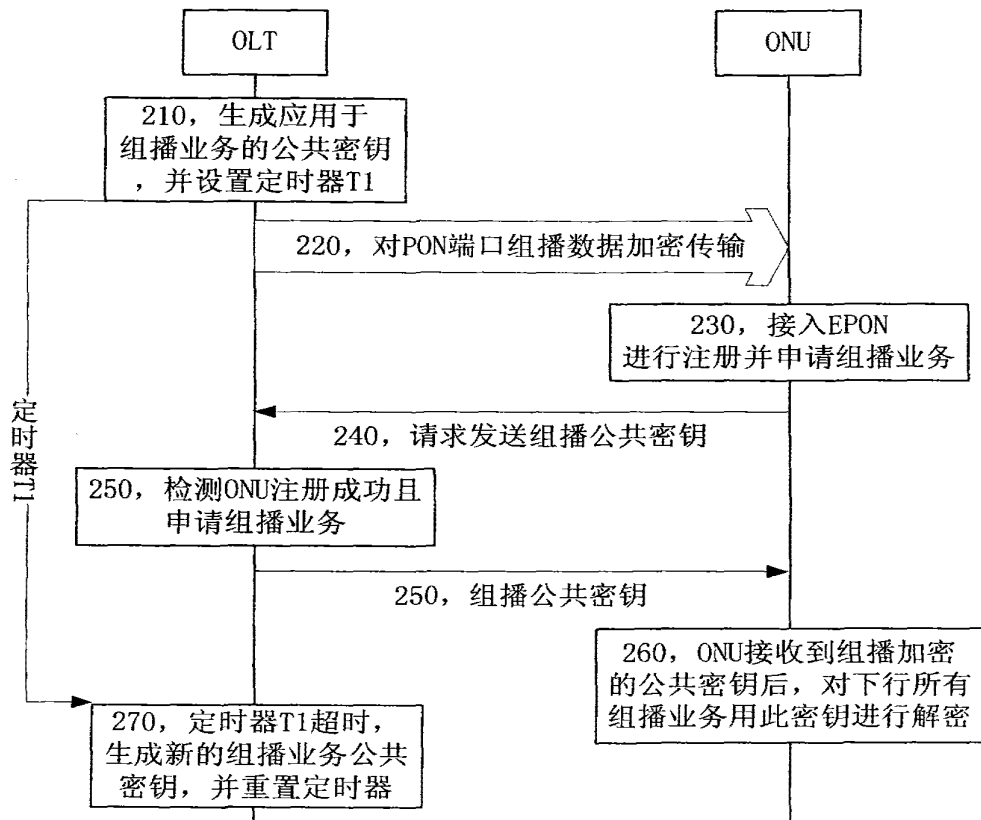


图 2

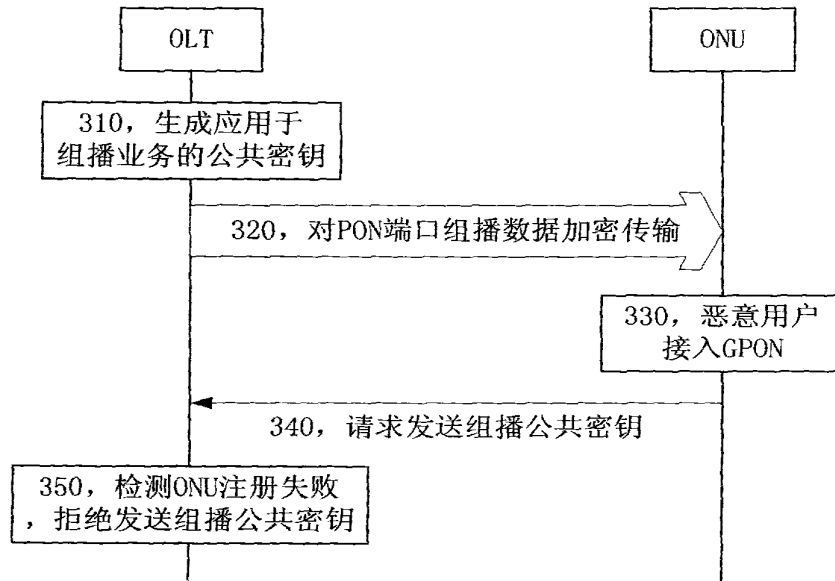


图 3

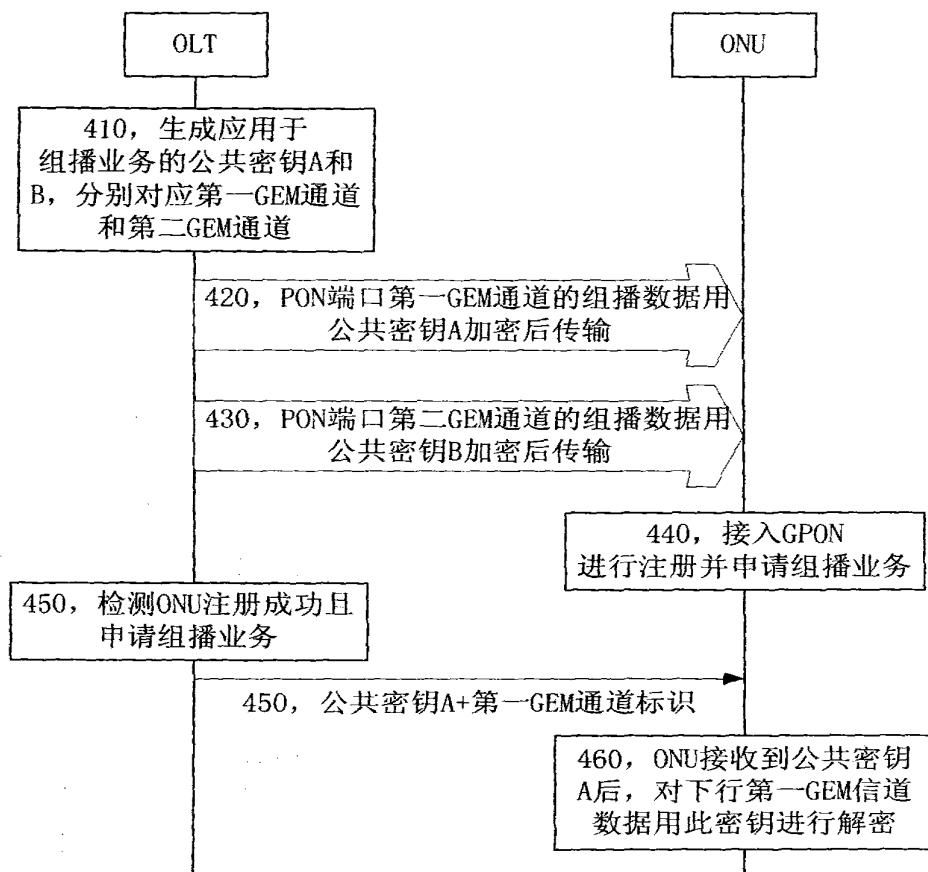


图 4

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



PCT



(10) 国际公布号

WO 2011/088700 A1

(43) 国际公布日
2011年7月28日 (28.07.2011)

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2010/078611

(22) 国际申请日: 2010年11月10日 (10.11.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010102646.2 2010年1月25日 (25.01.2010) CN

(71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 及

(75) 发明人/申请人 (仅对美国): **张德智 (ZHANG, Dezhi)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **袁立权 (YUAN, Liquan)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

(54) 发明名称: 一种无源光网络系统组播业务加密方法和装置

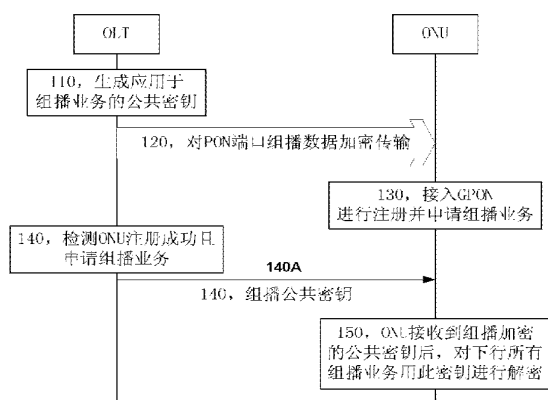


图1 / FIG. 1

(57) Abstract: A method for encrypting the multicast service in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generates a public key, transmits the multicast service data in a bearing channel after being encrypted using the public key, the multicast service data in the same bearing channel are encrypted using the same public key; and said OLT transmits the public key used to encrypt the multicast service data through a manage control channel to an Optical Network Unit (ONU) which has registered successfully and requested to receive said multicast service data. A device for encrypting the multicast service in a passive optical network system is also provided in the present invention. By applying the carrier channel encryption mechanism, the present invention is able to simplify the complexity of the OLT encryption mechanism and the ONU decryption mechanism, on the premise of ensuring the multicast service encryption.

[见续页]

- 110 GENERATING A PUBLIC KEY FOR THE MULTICAST SERVICE
120 ENCRYPTING AND TRANSMITTING THE MULTICAST DATA OF THE PON PORT
130 ACCESSING THE GPON, REGISTERING AND APPLYING THE MULTICAST SERVICE
140 DETECTING THE ONU HAVING REGISTERED SUCCESSFULLY AND HAVING APPLIED THE MULTICAST SERVICE
140A MULTICASTING THE PUBLIC KEY
150 AFTER RECEIVING THE PUBLIC KEY FOR ENCRYPTING THE MULTICAST, THE ONU DECRYPTS THE ENTIRE DOWNLINK MULTICAST SERVICE USING THE KEY



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种无源光网络系统组播业务加密方法,该方法包括:光线路终端(OLT)生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的组播业务数据使用相同的公共密钥加密;以及所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元(ONU)。本发明还公开了一种无源光网络系统组播业务加密装置。本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。

一种无源光网络系统组播业务加密方法和装置

技术领域

本发明涉及光通信领域，具体涉及一种用于无源光网络（Passive Optical Network, PON）系统中对组播业务数据进行加密的方法和装置。

背景技术

无源光网络的结构是一个 PON 口对应于多个 PON 终端用户光网络单元（Optical Network Unit, ONU）设备，且在下行链路上，每个用户 ONU 都能够接收局侧光线路终端（Optical Line Terminal, OLT）发出的所有数据。这里所说的“每个用户 ONU”包含合法用户和恶意用户两种情况：

拥有合法的注册信息，在物理连接到 PON 的某一根分支光纤后，可以和 OLT 交互消息进行注册，这种用户称之为合法用户；

不具有合法的注册信息，仅仅是在物理上连接到 PON 的某一根分支光纤，从不理会 OLT 发出的注册要求，仅接收下行信息，这种用户可以称之为恶意用户。

即使是合法用户，在其物理链接到一根分支光纤后，并在成功注册之前，也可以接收到 OLT PON 端口下发的各种明文数据包。目前 PON 技术中定义了一些加密机制，如吉比特无源光网络（Gigabit-Capable Passive Optical Network, GPON）系统的高级加密标准（Advanced Encryption Standard, AES）加密机制，或者以太网无源光网络（Ethernet Passive Optical Network, EPON）系统中的搅动加密机制和三重搅动加密机制等等，都是单播加密机制。对于组播数据（即 OLT PON 端口仅有一份业务数据下发，所有的用户或者符合要求的一部分用户接收并使用该业务数据），目前还没有有效的加密机制。一般运营商都是针对业务设置一个全网范围通用的密钥进行加密，但这种机制的缺点是一旦密钥被恶意用户得知，其全网所有业务内容都将被解密窃取。

运营商在 PON 中目前采用的方法是将组播业务数据包复制到每一个 PON 端口和用户 ONU 的单播通道上，应用单播机制进行加密，来保护组播

业务数据包不被恶意用户窃取。但是这种方法需要为每个 ONU 发送密钥，加重了 OLT 的负担。

发明内容

- 5 本发明要解决的技术问题是提供一种无源光网络系统组播业务加密方法和装置，提高安全性，简化 OLT 加密机制的复杂性，减轻 OLT 负荷。

为解决上述技术问题，本发明提供了一种无源光网络系统组播业务加密方法，该方法包括：

- 10 光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

所述方法还包括：

- 15 所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

所述方法还包括：

- 20 所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

- 25 OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请

接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

- 5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

为解决上述技术问题，本发明还提供了一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

- 10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

- 15 所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

- 25 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制,可以将密码泄露后的影响范围从全网限制到某一个 PON 口,提高了组播业务内容的安全性。

- 5 另外,通过对无源光网络承载的组播业务数据进行加密后传输,以及仅将密钥发送给注册成功的用户,使得恶意用户无法获知上述密钥,且合法用户在注册之前也无法得到密钥,从而防止恶意用户窃取组播业务内容的非法行为,同时不会影响合法用户在注册后正常使用加密后的组播业务。

10 附图概述

此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

图 1 为本发明实施例一的流程图;

- 15 图 2 为本发明实施例二的流程图;

图 3 为本发明实施例三的流程;

图 4 为本发明实施例四的流程图。

本发明的较佳实施方式

- 20 本发明的发明构思是:OLT 生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的数据使用相同的公共密钥加密;所述 OLT 通过管理控制通道(例如光网络单元管理与控制接口(Optical Network Terminal (ONT) Management Control Interface, OMCI)或者操作管理维护(Operation Administration Maintenance, OAM))将加密
- 25 组播业务数据时所采用的公共密钥(简称公钥)发送给注册成功的且申请接收所述组播业务数据的 ONU。

ONU 获取公共密钥后,使用该密钥对承载通道上该 ONU 申请接收的组

播业务数据进行解密。

- 优选地，OLT 定期维护该公钥，可以在生成公共密钥的同时为公共密钥设置老化时间（如通过定时器设置），待老化时间到达后，重新生成公共密钥并使用新生成的公共密钥加密承载通道上的组播业务数据，向注册成功的
- 5 且申请接收所述组播业务数据的 ONU 发送新生成的公共密钥。多个公共密钥的老化时间可以相同也可以不同。或者 OLT 也可以在任何需要的时候，更新该公共密钥。

- 所述承载通道是 PON 的逻辑通道，可以是 GPON 端口承载的通用封装格式（General Encapsulation Model, GEM）通道，或 EPON 端口的逻辑链路标识（Logical Link Identification, LLID）通道，且由 OLT 进行维护更新。
- 10

所述管理控制通道也是 PON 的逻辑通道，例如可以是 GPON 系统的物理层操作管理维护（Physical Layer Operation Administration Maintenance, PLOAM）通道或 OMCI 通道，或者 EPON 系统中的扩展 OAM 通道。或者，采用数据通道发送公共密钥。

- 15 OLT 可同时生成多个公共密钥，分别用于对不同的承载通道进行数据加密。优选的，同一 PON 端口下的各条承载通道的公共密钥可以相同也可以不同，例如，可以设置每条承载通道有不同的公共密钥，也可以使部分承载通道使用相同的公共密钥。

- 20 当 OLT 对多条承载通道上的组播数据进行加密，且该多条承载通道可能发送给相同的 ONU 时，可在向 ONU 发送公共密钥的同时将使用该公共密钥进行组播业务数据加密的承载通道的承载通道标识一并发送给 ONU，即将承载所述组播业务数据的承载通道的承载通道标识发送给 ONU，以便 ONU 解密。但也不排除 ONU 通过逐一解密的方法找到使用该公共密钥的承载通道。

- 25 下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

本实施例为 GPON 系统传送公共密钥的实施例，应用范围是整个 GPON 物理端口，如图 1 所示，流程包括：

步骤 110，OLT 生成应用于组播业务的公共密钥；

步骤 120，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

5 步骤 130，ONU 上电，接入 GPON 向 OLT 发起注册并申请组播业务；

关于具体的注册过程以及申请组播业务的过程，GPON 协议已经有相关定义，本文不再赘述。

步骤 140，OLT 检测该 ONU 注册成功且申请组播业务，将生成的公共密钥发送给该 ONU；

10 ONU 是否注册成功以及 ONU 申请何种组播业务在 OLT 上均有记录。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

OLT 可以采用 GPON 协议中的 PLOAM 通道，或者 OMCI 通道或其他通道（如数据通道）将组播公共密钥传递给注册成功的 ONU。

15 步骤 150，ONU 接收到组播加密的公共密钥后，对下行所有组播业务应用此密钥进行解密。

实施例二

20 本实施例为 EPON 系统传送公共密钥且进行密钥更新的实施例，应用范围是整个 EPON 物理端口，如图 2 所示，流程包括：

步骤 210，OLT 生成应用于组播业务的公共密钥，并为该公共密钥设定一个定时器 T1；

该定时器用于控制公共密钥的老化时间。

步骤 220，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

25 步骤 230，ONU 上电，接入 EPON 向 OLT 发起注册，并申请组播业务；

具体的注册过程以及申请组播业务的过程, EPON 协议已经有相关定义, 本文不再赘述。

步骤 240, ONU 请求 OLT 发送组播业务公共密钥;

步骤 250, OLT 接收到 ONU 的请求后, 查询该 ONU 如果处于注册成功
5 状态且该 ONU 申请组播业务, 则将生成的公共密钥发送给该 ONU;

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 260, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密;

10 步骤 270, 当 T1 定时器超时, OLT 重新生成新的公共密钥, 并重置 T1 定时器 (以便下次 T1 超时后再次更新密钥)。

当有其他 ONU 请求 OLT 发送组播业务公共密钥时, OLT 将新生成的公共密钥发送给请求公共密钥的 ONU。并且, OLT 还需要为已经发送过公共密钥的 ONU 更新公共密钥。

15 OLT 可以采用 EPON 系统中的管理控制通道 (如扩展 OAM 通道) 或数据通道将生成的组播公共密钥传递给注册成功的 ONU。

实施例三

本实施例为 GPON 系统中非法用户试图接入业务被拒绝的示例, 应用范
20 围是整个 GPON 物理端口, 如图 3 所示, 流程包括:

步骤 310, OLT 生成应用于组播业务的公共密钥;

步骤 320, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 330, 恶意用户 ONU 接入 GPON;

恶意用户接入 GPON 后可能不发起注册, 但如果发起注册的话必定无法
25 注册成功, 也无法申请组播业务。

步骤 340, 恶意用户 ONU 请求 OLT 发送组播业务公共密钥;

步骤 350, OLT 接收到请求后, 查询该 ONU 未能成功注册, 拒绝发送该组播公共密钥。

此时恶意 ONU 将无法获取组播公共密钥, 也就无法对组播业务内容进行解密, 运营商藉此防止了恶意用户的内容窃取。

实施例四

本实施例为 GPON 系统传送公共密钥的实施例, 应用范围是 GPON 物理端口中对应某一组播业务的一个 GEM 通道, 本实施例中的 ONU 仅申请了第一 GEM 通道上的组播业务, 如图 4 所示, 流程包括:

步骤 410, OLT 生成应用于第一 GEM 通道的组播公共密钥 A, 以及应用于第二 GEM 通道的组播公共密钥 B;

步骤 420, OLT 将承载在第一 GEM 通道的组播业务数据用公共密钥 A 加密后传输, 该通道所有 ONU 共享此公共密钥 A;

步骤 430, OLT 将承载在第二 GEM 通道的组播业务数据用公共密钥 B 加密后传输, 该通道所有 ONU 共享此公共密钥 B;

上述步骤 420 和 430 的执行顺序不固定。

步骤 440, ONU 上电, 接入 GPON 向 OLT 发起注册并申请组播业务;

步骤 450, OLT 检测到该 ONU 注册成功且申请接收的是第一 GEM 通道上的组播业务, 将该公共密钥 A 和对应的第一 GEM 通道标识传送给该 ONU;

在其他实施例中, 也可以由 ONU 主动发起密钥请求。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 460, ONU 接收到公共密钥 A 和对应的第一 GEM 通道标识后, 对第一 GEM 通道中传输的组播业务数据进行解密。

ONU1 未接收到公钥 B，无法解密下行第二 GEM 通道数据。可见，当同一 ONU 接收多个组播业务且该多个组播业务数据承载在不同的承载通道上时，OLT 需要在发送公钥的同时将该公钥对应的承载通道标识发送给该 ONU。

- 5 OLT 可以采用 GPON 协议中的 PLOAM 通道维护通道，或者 OMCI 管理通道或其他通道将组播公共密钥传递给注册成功的 ONU。

一个公共密钥可以用于一条 GEM 通道，也可以用于多条，即多条 GEM 通道共用一个密钥。

- 10 实现上述方法的 OLT 包括密钥生成单元、加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

- 15 所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

优选地，所述装置还包括：

老化时间设置单元，其设置为：对密钥生成单元生成的公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

- 25 所述发送单元还设置为：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

工业实用性

本发明通过采用承载通道加密机制，可以在保证组播业务加密的前提下，简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制，可以将密码泄露后的影响范围从全网限制到某一个 PON 口，提高了组播业务内容的安全性。

另外，通过对无源光网络承载的组播业务数据进行加密后传输，以及仅将密钥发送给注册成功的用户，使得恶意用户无法获知上述密钥，且合法用户在注册之前也无法得到密钥，从而防止恶意用户窃取组播业务内容的非法行为，同时不会影响合法用户在注册后正常使用加密后的组播业务。

权 利 要 求 书

1、一种无源光网络系统组播业务加密方法，该方法包括

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

5

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

2、如权利要求 1 所述的方法，其还包括：

所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

10

3、如权利要求 1 或 2 所述的方法，其还包括：

所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

15

4、如权利要求 1 所述的方法，其中：

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

20

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

5、如权利要求 1 所述的方法，其中：

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

6、如权利要求 1 或 2 所述的方法，其中：

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

7、一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 8、如权利要求 7 所述的装置，其中，

所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

9、如权利要求 7 所述的装置，其中：

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据

所采用的公共密钥发送给所述 ONU。

10、如权利要求 7 或 9 所述的装置，其中，

所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组
5 播业务数据加密的承载通道的承载通道标识。

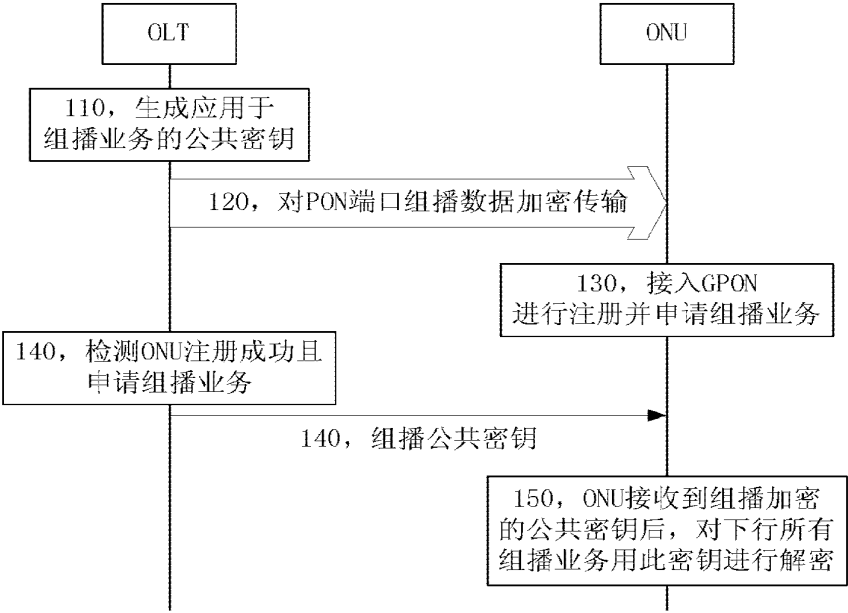


图 1

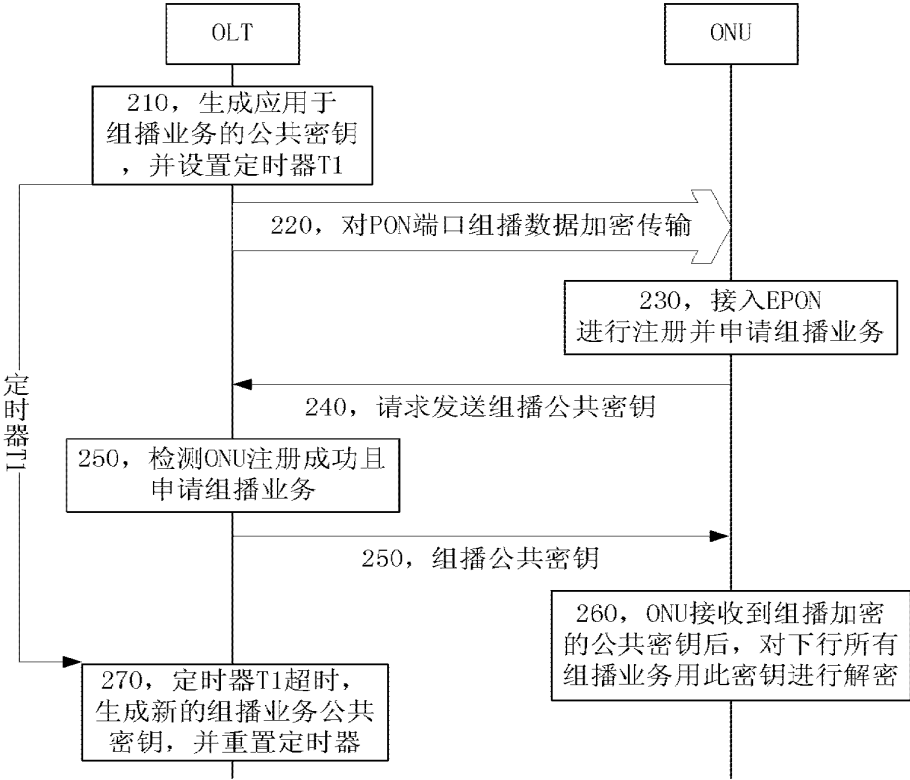


图 2

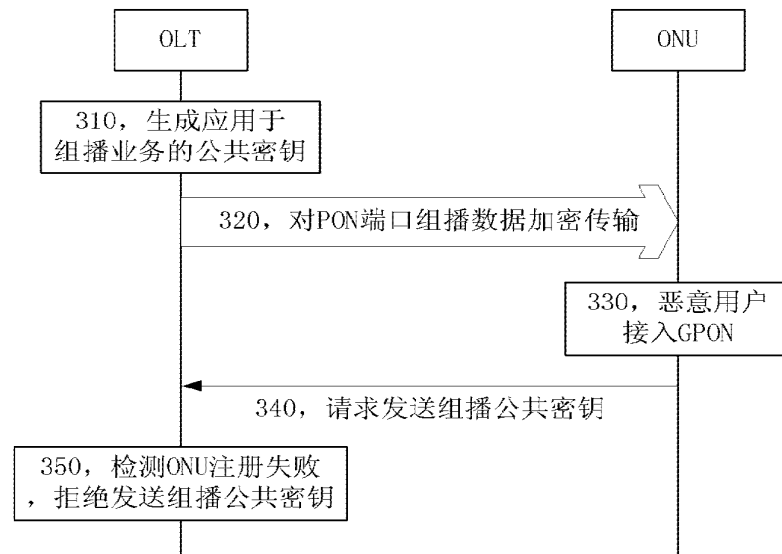


图 3

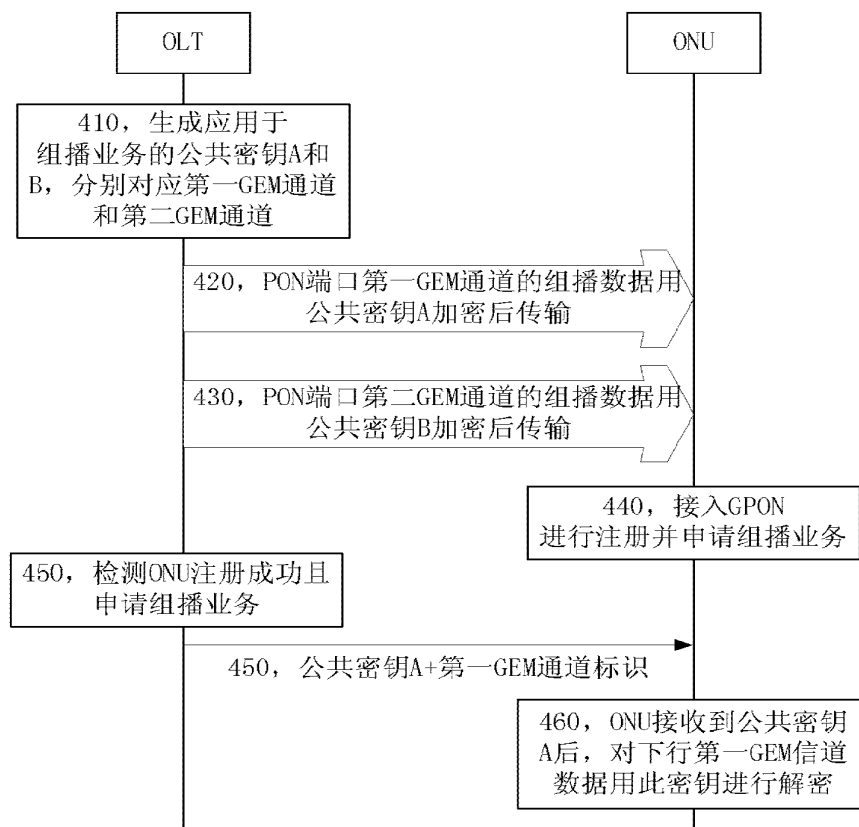


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/078611

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, H04J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CPRS, CPRSABS, WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1866857A (HUAWEI TECHNOLOGIES CO., LTD) 22 Nov. 2006(22.11.2006) Description pages 2, 5-6, Figs. 2-3	1-10
X	CN1855834A (HUAWEI TECHNOLOGIES CO., LTD) 01 Nov. 2006(01.11.2006) Description pages 4-5, Fig. 4	1-10
A	JP2000228668A (NEC CORP) 15 Aug. 2000(15.08.2000) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

21 Jan. 2011(21.01.2011)

Date of mailing of the international search report

17 Feb. 2011 (17.02.2011)Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer

WU, Weimin

Telephone No. (86-10)62411444

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/078611

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	NONE	
JP2000228668A	15.08.2000	NONE	

Form PCT/ISA /210 (patent family annex) (July 2009)

国际检索报告

 国际申请号
PCT/CN2010/078611

A. 主题的分类		
H04L 9/00 (2006.01) i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L, H04W, H04J		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNKI, CPRS, CPRSABS: 光网络, PON, EPON, GPON, OLT, ONU, ONT, 加密, 解密, 密钥, 公钥, 组播, 多播 WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN1866857A (华为技术有限公司) 22.11 月 2006(22.11.2006) 说明书 2, 5-6 页, 图 2-3	1-10
X	CN1855834A (华为技术有限公司) 01.11 月 2006(01.11.2006) 说明书 4-5 页, 图 4	1-10
A	JP2000228668A (NEC CORP) 15.8 月 2000(15.08.2000) 全文	1-10
☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件		“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件
国际检索实际完成的日期 21.1 月 2011(21.01.2011)		国际检索报告邮寄日期 17.2 月 2011 (17.02.2011)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 吴卫民 电话号码: (86-10) 62411444

PCT/ISA/210 表(第 2 页) (2009 年 7 月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/078611

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	无	
JP2000228668A	15.08.2000	无	

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)

Electronic Acknowledgement Receipt

EFS ID:	10989478
Application Number:	13257731
International Application Number:	PCT/CN10/78611
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi ZHANG
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	20-SEP-2011
Filing Date:	
Time Stamp:	14:43:34
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	sb0014_111101435-US.pdf	1348779 ca96f84568f79b179a156658c805ef0b438e b441	no	4

Warnings:

Information:

2	Documents submitted with 371 Applications	PCT_publication.pdf	884500 ab1d84e613d7201cb7466ddbc503bad29104c4ed	no	21
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	33238 aa009d9cf2a91cf4e2bd586a639c1089b5f35058	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2266517		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

- ☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Dezhi		ZHANG		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Shenzhen		Country Of Residenceⁱ	CN	
Citizenship under 37 CFR 1.41(b)ⁱ		CN			
Mailing Address of Applicant:					
Address 1	ZTE Plaza, Keji Road South,				
Address 2	Hi-Tech Industrial Park, Nanshan District,				
City	Shenzhen City, Guangdong Province		State/Province		
Postal Code	518057		Countryⁱ	CN	
Applicant 2					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Liquan		YUAN		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Shenzhen		Country Of Residenceⁱ	CN	
Citizenship under 37 CFR 1.41(b)ⁱ		CN			
Mailing Address of Applicant:					
Address 1	ZTE Plaza, Keji Road South,				
Address 2	Hi-Tech Industrial Park, Nanshan District,				
City	Shenzhen City, Guangdong Province		State/Province		
Postal Code	518057		Countryⁱ	CN	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					
Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		

☐ An Address is being provided for the correspondence information of this application.

Customer Number	95957		
Email Address	ling.wu@lingandyang.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		
Attorney Docket Number	AFD111101435-US	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	95957		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/CN2010/078611	2010-11-10
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			Remove
Application Number	Country ⁱ	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
201010102646.2	CN	2010-01-25	☒ Yes ☐ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.			
Assignee ¹			Remove
If the Assignee is an Organization check here. ☒			
Organization Name	ZTE CORPORATION		
Mailing Address Information:			
Address 1	ZTE Plaza, Keji Road South,		
Address 2	Hi-Tech Industrial Park, Nanshan District		
City	Shenzhen City, Guangdong Province ⁺	State/Province	
Country ⁱ	CN	Postal Code	518057
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature	/Ling Wu/		Date (YYYY-MM-DD)	2011-09-20	
First Name	Ling	Last Name	Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



PCT



(10) 国际公布号

WO 2011/088700 A1

(43) 国际公布日
2011年7月28日 (28.07.2011)

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2010/078611
- (22) 国际申请日: 2010年11月10日 (10.11.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201010102646.2 2010年1月25日 (25.01.2010) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **张德智 (ZHANG, Dezhi)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **袁立权 (YUAN, Liquan)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

(54) 发明名称: 一种无源光网络系统组播业务加密方法和装置

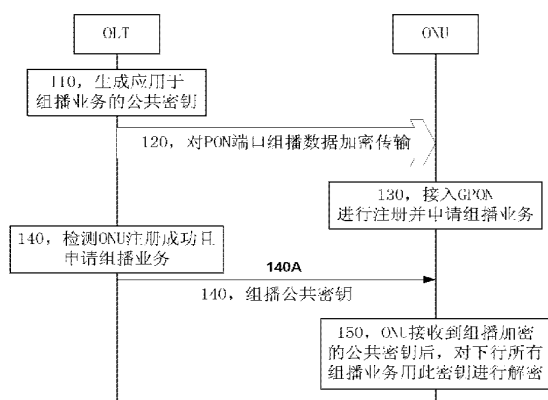


图1 / FIG. 1

(57) Abstract: A method for encrypting the multicast service in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generates a public key, transmits the multicast service data in a bearing channel after being encrypted using the public key, the multicast service data in the same bearing channel are encrypted using the same public key; and said OLT transmits the public key used to encrypt the multicast service data through a manage control channel to an Optical Network Unit (ONU) which has registered successfully and requested to receive said multicast service data. A device for encrypting the multicast service in a passive optical network system is also provided in the present invention. By applying the carrier channel encryption mechanism, the present invention is able to simplify the complexity of the OLT encryption mechanism and the ONU decryption mechanism, on the premise of ensuring the multicast service encryption.

[见续页]

- 110 GENERATING A PUBLIC KEY FOR THE MULTICAST SERVICE
120 ENCRYPTING AND TRANSMITTING THE MULTICAST DATA OF THE PON PORT
130 ACCESSING THE GPON, REGISTERING AND APPLYING THE MULTICAST SERVICE
140 DETECTING THE ONU HAVING REGISTERED SUCCESSFULLY AND HAVING APPLIED THE MULTICAST SERVICE
140A MULTICASTING THE PUBLIC KEY
150 AFTER RECEIVING THE PUBLIC KEY FOR ENCRYPTING THE MULTICAST, THE ONU DECRYPTS THE ENTIRE DOWNLINK MULTICAST SERVICE USING THE KEY

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种无源光网络系统组播业务加密方法,该方法包括:光线路终端(OLT)生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的组播业务数据使用相同的公共密钥加密;以及所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元(ONU)。本发明还公开了一种无源光网络系统组播业务加密装置。本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。

一种无源光网络系统组播业务加密方法和装置

技术领域

本发明涉及光通信领域，具体涉及一种用于无源光网络（Passive Optical Network, PON）系统中对组播业务数据进行加密的方法和装置。

背景技术

无源光网络的结构是一个 PON 口对应于多个 PON 终端用户光网络单元（Optical Network Unit, ONU）设备，且在下行链路上，每个用户 ONU 都能够接收局侧光线路终端（Optical Line Terminal, OLT）发出的所有数据。这里所说的“每个用户 ONU”包含合法用户和恶意用户两种情况：

拥有合法的注册信息，在物理连接到 PON 的某一根分支光纤后，可以和 OLT 交互消息进行注册，这种用户称之为合法用户；

不具有合法的注册信息，仅仅是在物理上连接到 PON 的某一根分支光纤，从不理会 OLT 发出的注册要求，仅接收下行信息，这种用户可以称之为恶意用户。

即使是合法用户，在其物理链接到一根分支光纤后，并在成功注册之前，也可以接收到 OLT PON 端口下发的各种明文数据包。目前 PON 技术中定义了一些加密机制，如吉比特无源光网络（Gigabit-Capable Passive Optical Network, GPON）系统的高级加密标准（Advanced Encryption Standard, AES）加密机制，或者以太网无源光网络（Ethernet Passive Optical Network, EPON）系统中的搅动加密机制和三重搅动加密机制等等，都是单播加密机制。对于组播数据（即 OLT PON 端口仅有一份业务数据下发，所有的用户或者符合要求的一部分用户接收并使用该业务数据），目前还没有有效的加密机制。一般运营商都是针对业务设置一个全网范围通用的密钥进行加密，但这种机制的缺点是一旦密钥被恶意用户得知，其全网所有业务内容都将被解密窃取。

运营商在 PON 中目前采用的方法是将组播业务数据包复制到每一个 PON 端口和用户 ONU 的单播通道上，应用单播机制进行加密，来保护组播

业务数据包不被恶意用户窃取。但是这种方法需要为每个 ONU 发送密钥，加重了 OLT 的负担。

发明内容

- 5 本发明要解决的技术问题是提供一种无源光网络系统组播业务加密方法和装置，提高安全性，简化 OLT 加密机制的复杂性，减轻 OLT 负荷。

为解决上述技术问题，本发明提供了一种无源光网络系统组播业务加密方法，该方法包括：

- 10 光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

所述方法还包括：

- 15 所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

所述方法还包括：

- 20 所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

- 25 OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请

接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

为解决上述技术问题，本发明还提供了一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

25 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制,可以将密码泄露后的影响范围从全网限制到某一个 PON 口,提高了组播业务内容的安全性。

- 5 另外,通过对无源光网络承载的组播业务数据进行加密后传输,以及仅将密钥发送给注册成功的用户,使得恶意用户无法获知上述密钥,且合法用户在注册之前也无法得到密钥,从而防止恶意用户窃取组播业务内容的非法行为,同时不会影响合法用户在注册后正常使用加密后的组播业务。

10 附图概述

此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

图 1 为本发明实施例一的流程图;

- 15 图 2 为本发明实施例二的流程图;

图 3 为本发明实施例三的流程;

图 4 为本发明实施例四的流程图。

本发明的较佳实施方式

- 20 本发明的发明构思是: OLT 生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的数据使用相同的公共密钥加密;所述 OLT 通过管理控制通道(例如光网络单元管理与控制接口(Optical Network Terminal (ONT) Management Control Interface, OMCI)或者操作管理维护(Operation Administration Maintenance, OAM))将加密
- 25 组播业务数据时所采用的公共密钥(简称公钥)发送给注册成功的且申请接收所述组播业务数据的 ONU。

ONU 获取公共密钥后,使用该密钥对承载通道上该 ONU 申请接收的组

播业务数据进行解密。

- 优选地，OLT 定期维护该公钥，可以在生成公共密钥的同时为公共密钥设置老化时间（如通过定时器设置），待老化时间到达后，重新生成公共密钥并使用新生成的公共密钥加密承载通道上的组播业务数据，向注册成功的
- 5 且申请接收所述组播业务数据的 ONU 发送新生成的公共密钥。多个公共密钥的老化时间可以相同也可以不同。或者 OLT 也可以在任何需要的时候，更新该公共密钥。

- 所述承载通道是 PON 的逻辑通道，可以是 GPON 端口承载的通用封装格式（General Encapsulation Model, GEM）通道，或 EPON 端口的逻辑链路
- 10 标识（Logical Link Identification, LLID）通道，且由 OLT 进行维护更新。

所述管理控制通道也是 PON 的逻辑通道，例如可以是 GPON 系统的物理层操作管理维护（Physical Layer Operation Administration Maintenance, PLOAM）通道或 OMCI 通道，或者 EPON 系统中的扩展 OAM 通道。或者，采用数据通道发送公共密钥。

- 15 OLT 可同时生成多个公共密钥，分别用于对不同的承载通道进行数据加密。优选的，同一 PON 端口下的各条承载通道的公共密钥可以相同也可以不同，例如，可以设置每条承载通道有不同的公共密钥，也可以使部分承载通道使用相同的公共密钥。

- 当 OLT 对多条承载通道上的组播数据进行加密，且该多条承载通道可能
- 20 发送给相同的 ONU 时，可在向 ONU 发送公共密钥的同时将使用该公共密钥进行组播业务数据加密的承载通道的承载通道标识一并发送给 ONU，即将承载所述组播业务数据的承载通道的承载通道标识发送给 ONU，以便 ONU 解密。但也不排除 ONU 通过逐一解密的方法找到使用该公共密钥的承载通道。

- 25 下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

本实施例为 GPON 系统传送公共密钥的实施例，应用范围是整个 GPON 物理端口，如图 1 所示，流程包括：

步骤 110，OLT 生成应用于组播业务的公共密钥；

步骤 120，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

5 步骤 130，ONU 上电，接入 GPON 向 OLT 发起注册并申请组播业务；

关于具体的注册过程以及申请组播业务的过程，GPON 协议已经有相关定义，本文不再赘述。

步骤 140，OLT 检测该 ONU 注册成功且申请组播业务，将生成的公共密钥发送给该 ONU；

10 ONU 是否注册成功以及 ONU 申请何种组播业务在 OLT 上均有记录。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

OLT 可以采用 GPON 协议中的 PLOAM 通道，或者 OMCI 通道或其他通道（如数据通道）将组播公共密钥传递给注册成功的 ONU。

15 步骤 150，ONU 接收到组播加密的公共密钥后，对下行所有组播业务应用此密钥进行解密。

实施例二

20 本实施例为 EPON 系统传送公共密钥且进行密钥更新的实施例，应用范围是整个 EPON 物理端口，如图 2 所示，流程包括：

步骤 210，OLT 生成应用于组播业务的公共密钥，并为该公共密钥设定一个定时器 T1；

该定时器用于控制公共密钥的老化时间。

步骤 220，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

25 步骤 230，ONU 上电，接入 EPON 向 OLT 发起注册，并申请组播业务；

具体的注册过程以及申请组播业务的过程, EPON 协议已经有相关定义, 本文不再赘述。

步骤 240, ONU 请求 OLT 发送组播业务公共密钥;

步骤 250, OLT 接收到 ONU 的请求后, 查询该 ONU 如果处于注册成功
5 状态且该 ONU 申请组播业务, 则将生成的公共密钥发送给该 ONU;

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 260, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密;

10 步骤 270, 当 T1 定时器超时, OLT 重新生成新的公共密钥, 并重置 T1 定时器 (以便下次 T1 超时后再次更新密钥)。

当有其他 ONU 请求 OLT 发送组播业务公共密钥时, OLT 将新生成的公共密钥发送给请求公共密钥的 ONU。并且, OLT 还需要为已经发送过公共密钥的 ONU 更新公共密钥。

15 OLT 可以采用 EPON 系统中的管理控制通道 (如扩展 OAM 通道) 或数据通道将生成的组播公共密钥传递给注册成功的 ONU。

实施例三

本实施例为 GPON 系统中非法用户试图接入业务被拒绝的示例, 应用范
20 围是整个 GPON 物理端口, 如图 3 所示, 流程包括:

步骤 310, OLT 生成应用于组播业务的公共密钥;

步骤 320, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 330, 恶意用户 ONU 接入 GPON;

恶意用户接入 GPON 后可能不发起注册, 但如果发起注册的话必定无法
25 注册成功, 也无法申请组播业务。

步骤 340, 恶意用户 ONU 请求 OLT 发送组播业务公共密钥;

步骤 350, OLT 接收到请求后, 查询该 ONU 未能成功注册, 拒绝发送该组播公共密钥。

此时恶意 ONU 将无法获取组播公共密钥, 也就无法对组播业务内容进行解密, 运营商藉此防止了恶意用户的内容窃取。

实施例四

本实施例为 GPON 系统传送公共密钥的实施例, 应用范围是 GPON 物理端口中对应某一组播业务的一个 GEM 通道, 本实施例中的 ONU 仅申请了第一 GEM 通道上的组播业务, 如图 4 所示, 流程包括:

步骤 410, OLT 生成应用于第一 GEM 通道的组播公共密钥 A, 以及应用于第二 GEM 通道的组播公共密钥 B;

步骤 420, OLT 将承载在第一 GEM 通道的组播业务数据用公共密钥 A 加密后传输, 该通道所有 ONU 共享此公共密钥 A;

步骤 430, OLT 将承载在第二 GEM 通道的组播业务数据用公共密钥 B 加密后传输, 该通道所有 ONU 共享此公共密钥 B;

上述步骤 420 和 430 的执行顺序不固定。

步骤 440, ONU 上电, 接入 GPON 向 OLT 发起注册并申请组播业务;

步骤 450, OLT 检测到该 ONU 注册成功且申请接收的是第一 GEM 通道上的组播业务, 将该公共密钥 A 和对应的第一 GEM 通道标识传送给该 ONU;

在其他实施例中, 也可以由 ONU 主动发起密钥请求。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 460, ONU 接收到公共密钥 A 和对应的第一 GEM 通道标识后, 对第一 GEM 通道中传输的组播业务数据进行解密。

ONU1 未接收到公钥 B，无法解密下行第二 GEM 通道数据。可见，当同一 ONU 接收多个组播业务且该多个组播业务数据承载在不同的承载通道上时，OLT 需要在发送公钥的同时将该公钥对应的承载通道标识发送给该 ONU。

- 5 OLT 可以采用 GPON 协议中的 PLOAM 通道维护通道，或者 OMCI 管理通道或其他通道将组播公共密钥传递给注册成功的 ONU。

一个公共密钥可以用于一条 GEM 通道，也可以用于多条，即多条 GEM 通道共用一个密钥。

- 10 实现上述方法的 OLT 包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

- 15 所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

优选地，所述装置还包括：

老化时间设置单元，其设置为：对密钥生成单元生成的公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

- 25 所述发送单元还设置为：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用5 硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和10 原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

工业实用性

本发明通过采用承载通道加密机制，可以在保证组播业务加密的前提下，15 简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制，可以将密码泄露后的影响范围从全网限制到某一个 PON 口，提高了组播业务内容的安全性。

另外，通过对无源光网络承载的组播业务数据进行加密后传输，以及仅将密钥发送给注册成功的用户，使得恶意用户无法获知上述密钥，且合法用20 户在注册之前也无法得到密钥，从而防止恶意用户窃取组播业务内容的非法行为，同时不会影响合法用户在注册后正常使用加密后的组播业务。

权 利 要 求 书

1、一种无源光网络系统组播业务加密方法，该方法包括

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

2、如权利要求 1 所述的方法，其还包括：

所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

3、如权利要求 1 或 2 所述的方法，其还包括：

所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

4、如权利要求 1 所述的方法，其中：

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

5、如权利要求 1 所述的方法，其中：

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

6、如权利要求 1 或 2 所述的方法，其中：

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

7、一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 8、如权利要求 7 所述的装置，其中，

所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

9、如权利要求 7 所述的装置，其中：

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据

所采用的公共密钥发送给所述 ONU。

10、如权利要求 7 或 9 所述的装置，其中，

所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

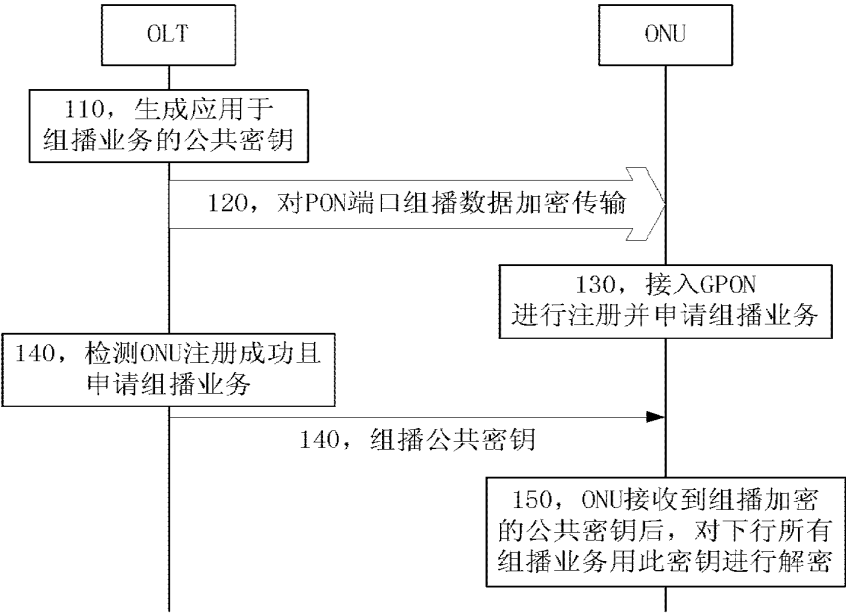


图 1

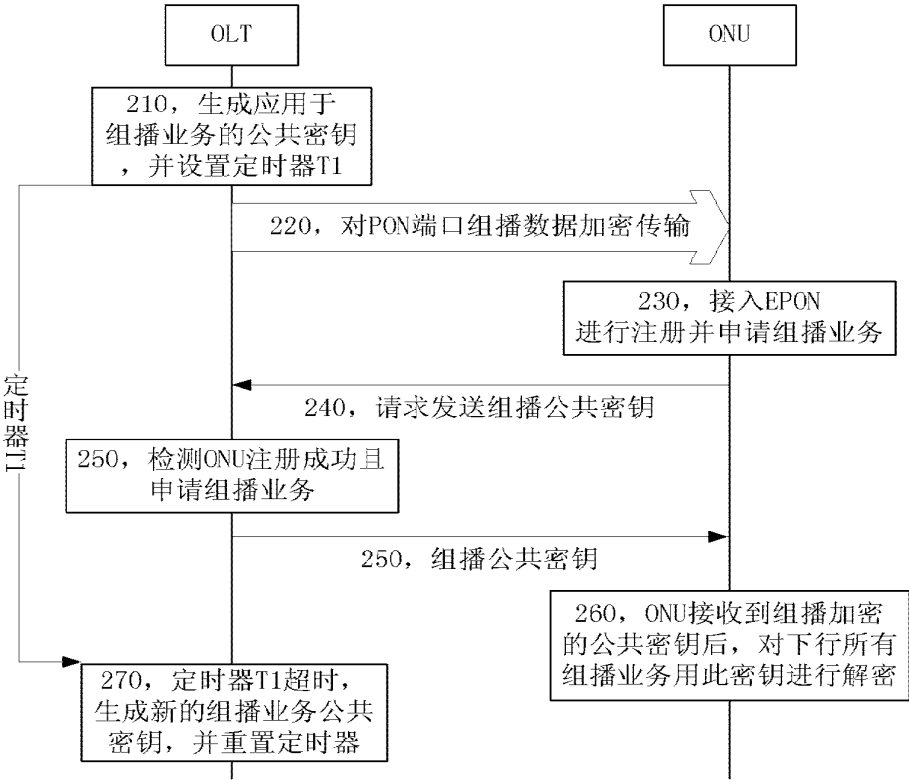


图 2

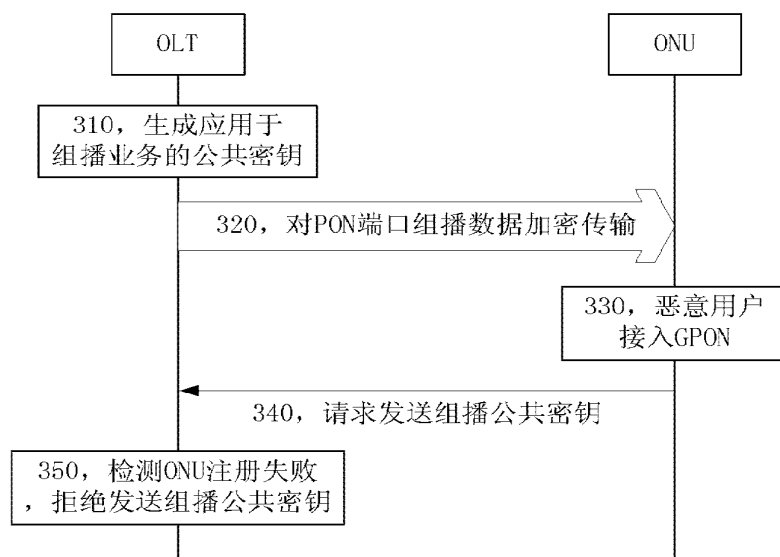


图 3

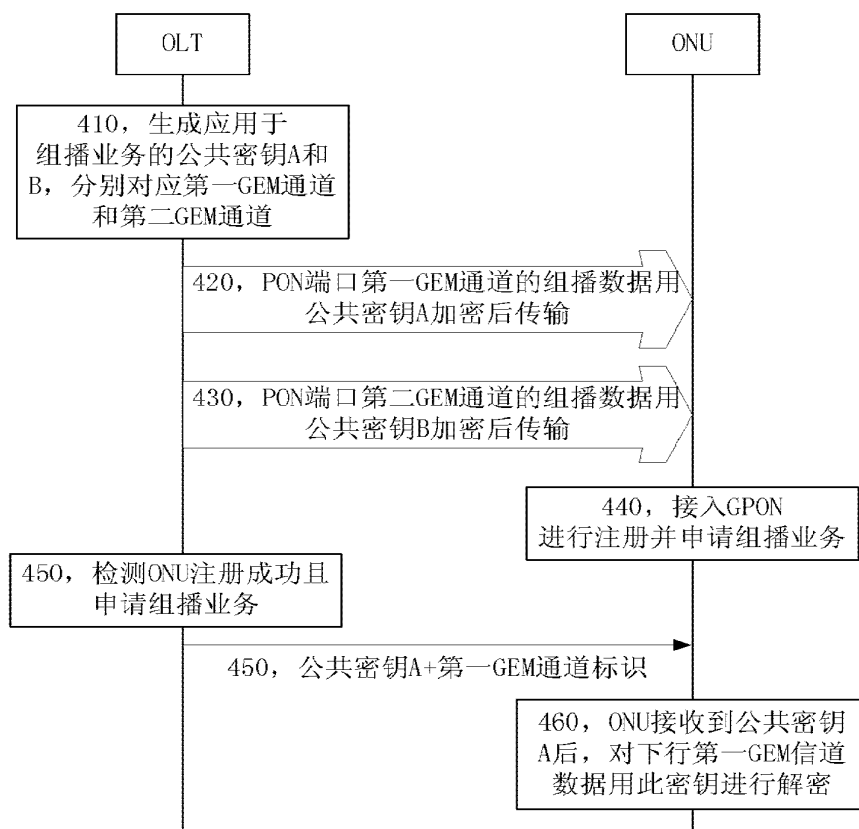


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/078611

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, H04J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CPRS, CPRSABS, WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrvpt+, cipher+, decrypt+, kev, public w kev, multicast+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1866857A (HUAWEI TECHNOLOGIES CO., LTD) 22 Nov. 2006(22.11.2006) Description pages 2, 5-6, Figs. 2-3	1-10
X	CN1855834A (HUAWEI TECHNOLOGIES CO., LTD) 01 Nov. 2006(01.11.2006) Description pages 4-5, Fig. 4	1-10
A	JP2000228668A (NEC CORP) 15 Aug. 2000(15.08.2000) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

21 Jan. 2011(21.01.2011)

Date of mailing of the international search report

17 Feb. 2011 (17.02.2011)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer

WU, Weimin

Telephone No. (86-10)62411444

International application No.
PCT/CN2010/078611

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	NONE	
JP2000228668A	15.08.2000	NONE	

国际检索报告

国际申请号
PCT/CN2010/078611

A. 主题的分类		
H04L 9/00 (2006.01) i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L, H04W, H04J		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNKI, CPRS, CPRSABS:光网络, PON, EPON, GPON, OLT, ONU, ONT, 加密, 解密, 密钥, 公钥, 组播, 多播 WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN1866857A (华为技术有限公司) 22.11 月 2006(22.11.2006) 说明书 2, 5-6 页, 图 2-3	1-10
X	CN1855834A (华为技术有限公司) 01.11 月 2006(01.11.2006) 说明书 4-5 页, 图 4	1-10
A	JP2000228668A (NEC CORP) 15.8 月 2000(15.08.2000) 全文	1-10
☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 21.1 月 2011(21.01.2011)		国际检索报告邮寄日期 17.2 月 2011 (17.02.2011)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		受权官员 吴卫民 电话号码: (86-10) 62411444

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/078611

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	无	
JP2000228668A	15.08.2000	无	

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Method and Device for Encrypting Multicast Service in Passive Optical Network System		
First Named Inventor/Applicant Name:		Dezhi ZHANG		
Filer:		Ling Wu		
Attorney Docket Number:		AFD111101435-US		
Filed as Large Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
National Stage Fee	1631	1	330	330
Natl Stage Search Fee - Report provided	1642	1	430	430
National Stage Exam - all other cases	1633	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				980

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

- ☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Dezhi		ZHANG		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Shenzhen		Country Of Residenceⁱ	CN	
Citizenship under 37 CFR 1.41(b)ⁱ		CN			
Mailing Address of Applicant:					
Address 1	ZTE Plaza, Keji Road South,				
Address 2	Hi-Tech Industrial Park, Nanshan District,				
City	Shenzhen City, Guangdong Province		State/Province		
Postal Code	518057		Countryⁱ	CN	
Applicant 2					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Liquan		YUAN		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Shenzhen		Country Of Residenceⁱ	CN	
Citizenship under 37 CFR 1.41(b)ⁱ		CN			
Mailing Address of Applicant:					
Address 1	ZTE Plaza, Keji Road South,				
Address 2	Hi-Tech Industrial Park, Nanshan District,				
City	Shenzhen City, Guangdong Province		State/Province		
Postal Code	518057		Countryⁱ	CN	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					
Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		

☐ An Address is being provided for the correspondence information of this application.

Customer Number	95957		
Email Address	ling.wu@lingandyang.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		
Attorney Docket Number	AFD111101435-US	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	95957		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/CN2010/078611	2010-11-10
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	AFD111101435-US
		Application Number	
Title of Invention	Method and Device for Encrypting Multicast Service in Passive Optical Network System		

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			Remove
Application Number	Country ⁱ	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
201010102646.2	CN	2010-01-25	☒ Yes ☐ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.			
Assignee ¹			Remove
If the Assignee is an Organization check here. ☒			
Organization Name	ZTE CORPORATION		
Mailing Address Information:			
Address 1	ZTE Plaza, Keji Road South,		
Address 2	Hi-Tech Industrial Park, Nanshan District		
City	Shenzhen City, Guangdong Province ⁺	State/Province	
Country ⁱ	CN	Postal Code	518057
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature	/Ling Wu/		Date (YYYY-MM-DD)	2011-09-20	
First Name	Ling	Last Name	Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	10990063
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi ZHANG
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	20-SEP-2011
Filing Date:	
Time Stamp:	15:04:38
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 980
RAM confirmation Number	1738
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Application Data Sheet	sb0014_111101435-US.pdf	1348779 ca96f84568f79b179a156658c805ef0b438eb441	no	4
Warnings:					
Information:					
2	Documents submitted with 371 Applications	PCT_publication.pdf	884500 ab1d84e613d7201cb7466ddbc503bad29104c4ed	no	21
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	35270 e77154fca9d6cf5b9a829ccc2822169bbd287543	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2268549		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Electronic Patent Application Fee Transmittal				
Application Number:		13257731		
Filing Date:				
Title of Invention:		Method and Device for Encrypting Multicast Service in Passive Optical Network System		
First Named Inventor/Applicant Name:		Dezhi ZHANG		
Filer:		Ling Wu		
Attorney Docket Number:		AFD111101435-US		
Filed as Large Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
National Stage Fee	1631	1	330	330
Natl Stage Search Fee - Report provided	1642	1	430	430
National Stage Exam - all other cases	1633	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				980

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



PCT



(10) 国际公布号

WO 2011/088700 A1

(43) 国际公布日
2011年7月28日 (28.07.2011)

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2010/078611
- (22) 国际申请日: 2010年11月10日 (10.11.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201010102646.2 2010年1月25日 (25.01.2010) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **张德智 (ZHANG, Dezhi)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **袁立权 (YUAN, Liquan)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

(54) 发明名称: 一种无源光网络系统组播业务加密方法和装置

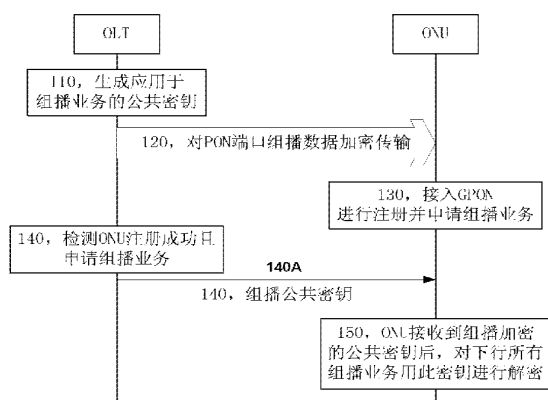


图1 / FIG. 1

(57) Abstract: A method for encrypting the multicast service in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generates a public key, transmits the multicast service data in a bearing channel after being encrypted using the public key, the multicast service data in the same bearing channel are encrypted using the same public key; and said OLT transmits the public key used to encrypt the multicast service data through a manage control channel to an Optical Network Unit (ONU) which has registered successfully and requested to receive said multicast service data. A device for encrypting the multicast service in a passive optical network system is also provided in the present invention. By applying the carrier channel encryption mechanism, the present invention is able to simplify the complexity of the OLT encryption mechanism and the ONU decryption mechanism, on the premise of ensuring the multicast service encryption.

[见续页]

- 110 GENERATING A PUBLIC KEY FOR THE MULTICAST SERVICE
120 ENCRYPTING AND TRANSMITTING THE MULTICAST DATA OF THE PON PORT
130 ACCESSING THE GPON, REGISTERING AND APPLYING THE MULTICAST SERVICE
140 DETECTING THE ONU HAVING REGISTERED SUCCESSFULLY AND HAVING APPLIED THE MULTICAST SERVICE
140A MULTICASTING THE PUBLIC KEY
150 AFTER RECEIVING THE PUBLIC KEY FOR ENCRYPTING THE MULTICAST, THE ONU DECRYPTS THE ENTIRE DOWNLINK MULTICAST SERVICE USING THE KEY

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种无源光网络系统组播业务加密方法,该方法包括:光线路终端(OLT)生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的组播业务数据使用相同的公共密钥加密;以及所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元(ONU)。本发明还公开了一种无源光网络系统组播业务加密装置。本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。

一种无源光网络系统组播业务加密方法和装置

技术领域

本发明涉及光通信领域，具体涉及一种用于无源光网络（Passive Optical
5 Network, PON）系统中对组播业务数据进行加密的方法和装置。

背景技术

无源光网络的结构是一个 PON 口对应于多个 PON 终端用户光网络单元
（Optical Network Unit, ONU）设备，且在下行链路上，每个用户 ONU 都
10 能够接收局侧光线路终端（Optical Line Terminal, OLT）发出的所有数据。
这里所说的“每个用户 ONU”包含合法用户和恶意用户两种情况：

拥有合法的注册信息，在物理连接到 PON 的某一根分支光纤后，可以和
OLT 交互消息进行注册，这种用户称之为合法用户；

不具有合法的注册信息，仅仅是在物理上连接到 PON 的某一根分支光
15 纤，从不理会 OLT 发出的注册要求，仅接收下行信息，这种用户可以称之为
恶意用户。

即使是合法用户，在其物理链接到一根分支光纤后，并在成功注册之前，
也可以接收到 OLT PON 端口下发的各种明文数据包。目前 PON 技术中定义
了一些加密机制，如吉比特无源光网络（Gigabit-Capable Passive Optical
20 Network, GPON）系统的高级加密标准（Advanced Encryption Standard, AES）
加密机制，或者以太网无源光网络（Ethernet Passive Optical Network, EPON）
系统中的搅动加密机制和三重搅动加密机制等等，都是单播加密机制。对于
组播数据（即 OLT PON 端口仅有一份业务数据下发，所有的用户或者符合
要求的一部分用户接收并使用该业务数据），目前还没有有效的加密机制。
25 一般运营商都是针对业务设置一个全网范围通用的密钥进行加密，但这种机
制的缺点是一旦密钥被恶意用户得知，其全网所有业务内容都将被解密窃取。

运营商在 PON 中目前采用的方法是将组播业务数据包复制到每一个
PON 端口和用户 ONU 的单播通道上，应用单播机制进行加密，来保护组播

业务数据包不被恶意用户窃取。但是这种方法需要为每个 ONU 发送密钥，加重了 OLT 的负担。

发明内容

- 5 本发明要解决的技术问题是提供一种无源光网络系统组播业务加密方法和装置，提高安全性，简化 OLT 加密机制的复杂性，减轻 OLT 负荷。

为解决上述技术问题，本发明提供了一种无源光网络系统组播业务加密方法，该方法包括：

- 10 光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

所述方法还包括：

- 15 所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

所述方法还包括：

- 20 所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

- 25 OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请

接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

为解决上述技术问题，本发明还提供了一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

25 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制,可以将密码泄露后的影响范围从全网限制到某一个 PON 口,提高了组播业务内容的安全性。

- 5 另外,通过对无源光网络承载的组播业务数据进行加密后传输,以及仅将密钥发送给注册成功的用户,使得恶意用户无法获知上述密钥,且合法用户在注册之前也无法得到密钥,从而防止恶意用户窃取组播业务内容的非法行为,同时不会影响合法用户在注册后正常使用加密后的组播业务。

10 附图概述

此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

图 1 为本发明实施例一的流程图;

- 15 图 2 为本发明实施例二的流程图;

图 3 为本发明实施例三的流程;

图 4 为本发明实施例四的流程图。

本发明的较佳实施方式

- 20 本发明的发明构思是: OLT 生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的数据使用相同的公共密钥加密;所述 OLT 通过管理控制通道(例如光网络单元管理与控制接口(Optical Network Terminal (ONT) Management Control Interface, OMCI)或者操作管理维护(Operation Administration Maintenance, OAM))将加密
- 25 组播业务数据时所采用的公共密钥(简称公钥)发送给注册成功的且申请接收所述组播业务数据的 ONU。

ONU 获取公共密钥后,使用该密钥对承载通道上该 ONU 申请接收的组

播业务数据进行解密。

- 优选地，OLT 定期维护该公钥，可以在生成公共密钥的同时为公共密钥设置老化时间（如通过定时器设置），待老化时间到达后，重新生成公共密钥并使用新生成的公共密钥加密承载通道上的组播业务数据，向注册成功的
- 5 且申请接收所述组播业务数据的 ONU 发送新生成的公共密钥。多个公共密钥的老化时间可以相同也可以不同。或者 OLT 也可以在任何需要的时候，更新该公共密钥。

- 所述承载通道是 PON 的逻辑通道，可以是 GPON 端口承载的通用封装格式（General Encapsulation Model, GEM）通道，或 EPON 端口的逻辑链路标识（Logical Link Identification, LLID）通道，且由 OLT 进行维护更新。
- 10

所述管理控制通道也是 PON 的逻辑通道，例如可以是 GPON 系统的物理层操作管理维护（Physical Layer Operation Administration Maintenance, PLOAM）通道或 OMCI 通道，或者 EPON 系统中的扩展 OAM 通道。或者，采用数据通道发送公共密钥。

- 15 OLT 可同时生成多个公共密钥，分别用于对不同的承载通道进行数据加密。优选的，同一 PON 端口下的各条承载通道的公共密钥可以相同也可以不同，例如，可以设置每条承载通道有不同的公共密钥，也可以使部分承载通道使用相同的公共密钥。

- 20 当 OLT 对多条承载通道上的组播数据进行加密，且该多条承载通道可能发送给相同的 ONU 时，可在向 ONU 发送公共密钥的同时将使用该公共密钥进行组播业务数据加密的承载通道的承载通道标识一并发送给 ONU，即将承载所述组播业务数据的承载通道的承载通道标识发送给 ONU，以便 ONU 解密。但也不排除 ONU 通过逐一解密的方法找到使用该公共密钥的承载通道。

- 25 下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

本实施例为 GPON 系统传送公共密钥的实施例，应用范围是整个 GPON 物理端口，如图 1 所示，流程包括：

步骤 110，OLT 生成应用于组播业务的公共密钥；

步骤 120，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

5 步骤 130，ONU 上电，接入 GPON 向 OLT 发起注册并申请组播业务；

关于具体的注册过程以及申请组播业务的过程，GPON 协议已经有相关定义，本文不再赘述。

步骤 140，OLT 检测该 ONU 注册成功且申请组播业务，将生成的公共密钥发送给该 ONU；

10 ONU 是否注册成功以及 ONU 申请何种组播业务在 OLT 上均有记录。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

OLT 可以采用 GPON 协议中的 PLOAM 通道，或者 OMCI 通道或其他通道（如数据通道）将组播公共密钥传递给注册成功的 ONU。

15 步骤 150，ONU 接收到组播加密的公共密钥后，对下行所有组播业务应用此密钥进行解密。

实施例二

20 本实施例为 EPON 系统传送公共密钥且进行密钥更新的实施例，应用范围是整个 EPON 物理端口，如图 2 所示，流程包括：

步骤 210，OLT 生成应用于组播业务的公共密钥，并为该公共密钥设定一个定时器 T1；

该定时器用于控制公共密钥的老化时间。

步骤 220，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

25 步骤 230，ONU 上电，接入 EPON 向 OLT 发起注册，并申请组播业务；

具体的注册过程以及申请组播业务的过程, EPON 协议已经有相关定义, 本文不再赘述。

步骤 240, ONU 请求 OLT 发送组播业务公共密钥;

步骤 250, OLT 接收到 ONU 的请求后, 查询该 ONU 如果处于注册成功
5 状态且该 ONU 申请组播业务, 则将生成的公共密钥发送给该 ONU;

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 260, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密;

10 步骤 270, 当 T1 定时器超时, OLT 重新生成新的公共密钥, 并重置 T1 定时器 (以便下次 T1 超时后再次更新密钥)。

当有其他 ONU 请求 OLT 发送组播业务公共密钥时, OLT 将新生成的公共密钥发送给请求公共密钥的 ONU。并且, OLT 还需要为已经发送过公共密钥的 ONU 更新公共密钥。

15 OLT 可以采用 EPON 系统中的管理控制通道 (如扩展 OAM 通道) 或数据通道将生成的组播公共密钥传递给注册成功的 ONU。

实施例三

本实施例为 GPON 系统中非法用户试图接入业务被拒绝的示例, 应用范
20 围是整个 GPON 物理端口, 如图 3 所示, 流程包括:

步骤 310, OLT 生成应用于组播业务的公共密钥;

步骤 320, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 330, 恶意用户 ONU 接入 GPON;

恶意用户接入 GPON 后可能不发起注册, 但如果发起注册的话必定无法
25 注册成功, 也无法申请组播业务。

步骤 340, 恶意用户 ONU 请求 OLT 发送组播业务公共密钥;

步骤 350, OLT 接收到请求后, 查询该 ONU 未能成功注册, 拒绝发送该组播公共密钥。

此时恶意 ONU 将无法获取组播公共密钥, 也就无法对组播业务内容进行解密, 运营商藉此防止了恶意用户的内容窃取。

实施例四

本实施例为 GPON 系统传送公共密钥的实施例, 应用范围是 GPON 物理端口中对应某一组播业务的一个 GEM 通道, 本实施例中的 ONU 仅申请了第一 GEM 通道上的组播业务, 如图 4 所示, 流程包括:

步骤 410, OLT 生成应用于第一 GEM 通道的组播公共密钥 A, 以及应用于第二 GEM 通道的组播公共密钥 B;

步骤 420, OLT 将承载在第一 GEM 通道的组播业务数据用公共密钥 A 加密后传输, 该通道所有 ONU 共享此公共密钥 A;

步骤 430, OLT 将承载在第二 GEM 通道的组播业务数据用公共密钥 B 加密后传输, 该通道所有 ONU 共享此公共密钥 B;

上述步骤 420 和 430 的执行顺序不固定。

步骤 440, ONU 上电, 接入 GPON 向 OLT 发起注册并申请组播业务;

步骤 450, OLT 检测到该 ONU 注册成功且申请接收的是第一 GEM 通道上的组播业务, 将该公共密钥 A 和对应的第一 GEM 通道标识发送给该 ONU;

在其他实施例中, 也可以由 ONU 主动发起密钥请求。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 460, ONU 接收到公共密钥 A 和对应的第一 GEM 通道标识后, 对第一 GEM 通道中传输的组播业务数据进行解密。

ONU1 未接收到公钥 B, 无法解密下行第二 GEM 通道数据。可见, 当同一 ONU 接收多个组播业务且该多个组播业务数据承载在不同的承载通道上时, OLT 需要在发送公钥的同时将该公钥对应的承载通道标识发送给该 ONU。

- 5 OLT 可以采用 GPON 协议中的 PLOAM 通道维护通道, 或者 OMCI 管理通道或其他通道将组播公共密钥传递给注册成功的 ONU。

一个公共密钥可以用于一条 GEM 通道, 也可以用于多条, 即多条 GEM 通道共用一个密钥。

- 10 实现上述方法的 OLT 包括密钥生成单元, 加密单元以及发送单元, 其中:

所述密钥生成单元设置为: 生成公共密钥;

所述加密单元设置为: 对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密;

- 15 所述发送单元设置为: 发送加密后的组播业务数据, 以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

优选地, 所述装置还包括:

老化时间设置单元, 其设置为: 对密钥生成单元生成的公共密钥设置老化时间, 当老化时间到达时, 通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元还设置为: 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时, 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

- 25 所述发送单元还设置为: 判断 ONU 注册成功且申请接收组播业务数据后, 主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU; 或者, 在接收到 ONU 请求密钥的请求后, 判断所述 ONU 注册成功且申请接收组播业务数据, 则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用5 硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和10 原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

工业实用性

本发明通过采用承载通道加密机制，可以在保证组播业务加密的前提下，15 简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制，可以将密码泄露后的影响范围从全网限制到某一个 PON 口，提高了组播业务内容的安全性。

另外，通过对无源光网络承载的组播业务数据进行加密后传输，以及仅将密钥发送给注册成功的用户，使得恶意用户无法获知上述密钥，且合法用20 户在注册之前也无法得到密钥，从而防止恶意用户窃取组播业务内容的非法行为，同时不会影响合法用户在注册后正常使用加密后的组播业务。

权 利 要 求 书

1、一种无源光网络系统组播业务加密方法，该方法包括

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

2、如权利要求 1 所述的方法，其还包括：

所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

3、如权利要求 1 或 2 所述的方法，其还包括：

所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

4、如权利要求 1 所述的方法，其中：

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

5、如权利要求 1 所述的方法，其中：

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

6、如权利要求 1 或 2 所述的方法，其中：

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

7、一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 8、如权利要求 7 所述的装置，其中，

所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

9、如权利要求 7 所述的装置，其中：

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据

所采用的公共密钥发送给所述 ONU。

10、如权利要求 7 或 9 所述的装置，其中，

所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

5

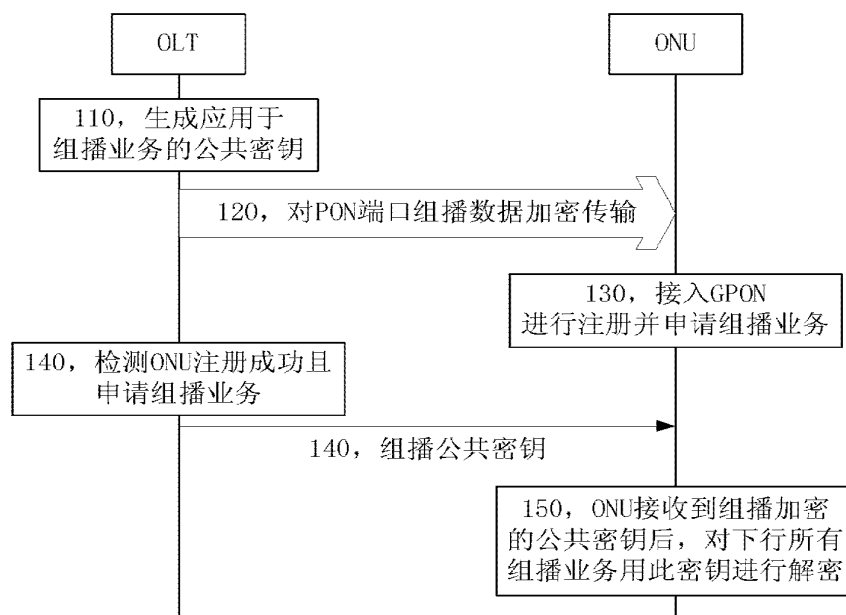


图 1

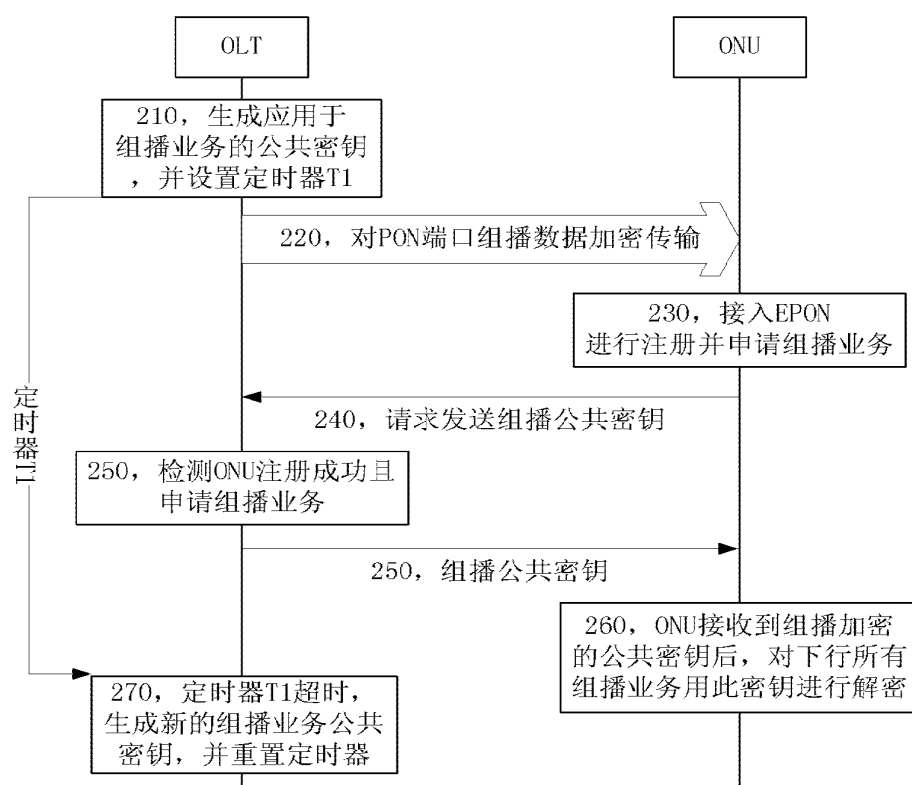


图 2

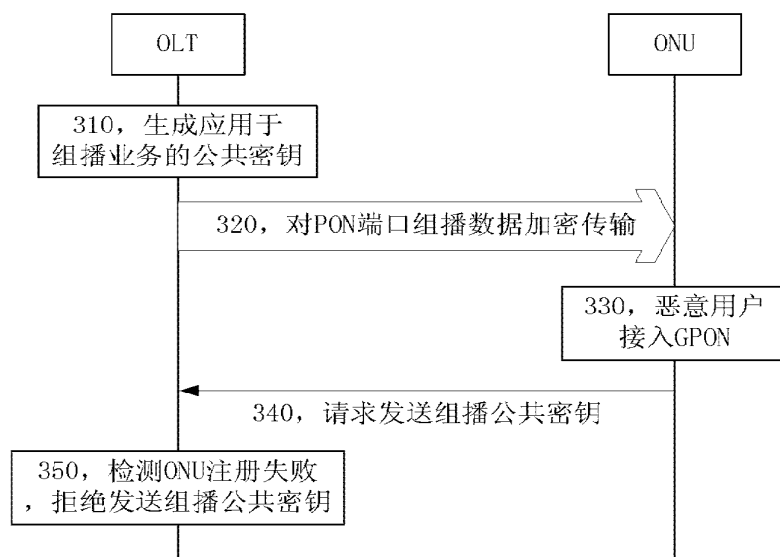


图 3

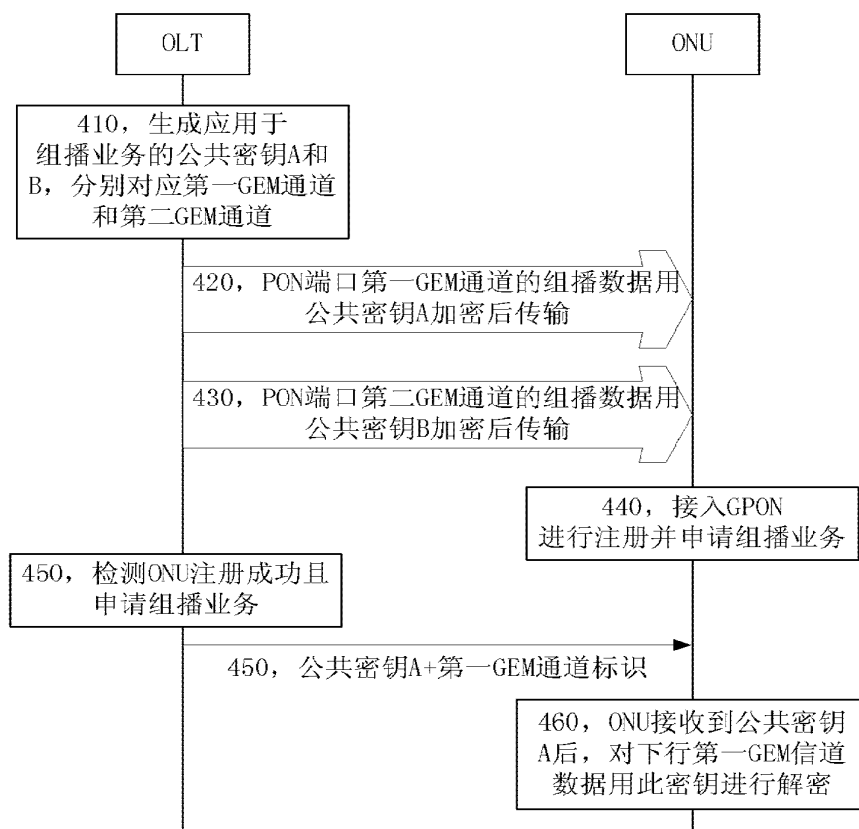


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/078611

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, H04J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CPRS, CPRSABS, WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrvpt+, cipher+, decrypt+, key, public w key, multicast+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1866857A (HUAWEI TECHNOLOGIES CO., LTD) 22 Nov. 2006(22.11.2006) Description pages 2, 5-6, Figs. 2-3	1-10
X	CN1855834A (HUAWEI TECHNOLOGIES CO., LTD) 01 Nov. 2006(01.11.2006) Description pages 4-5, Fig. 4	1-10
A	JP2000228668A (NEC CORP) 15 Aug. 2000(15.08.2000) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

21 Jan. 2011(21.01.2011)

Date of mailing of the international search report

17 Feb. 2011 (17.02.2011)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer

WU, Weimin

Telephone No. (86-10)62411444

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2010/078611

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	NONE	
JP2000228668A	15.08.2000	NONE	

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号
PCT/CN2010/078611

A. 主题的分类		
H04L 9/00 (2006.01) i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L, H04W, H04J		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNKI, CPRS, CPRSABS:光网络, PON, EPON, GPON, OLT, ONU, ONT, 加密, 解密, 密钥, 公钥, 组播, 多播 WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN1866857A (华为技术有限公司) 22.11 月 2006(22.11.2006) 说明书 2, 5-6 页, 图 2-3	1-10
X	CN1855834A (华为技术有限公司) 01.11 月 2006(01.11.2006) 说明书 4-5 页, 图 4	1-10
A	JP2000228668A (NEC CORP) 15.8 月 2000(15.08.2000) 全文	1-10
☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 21.1 月 2011(21.01.2011)		国际检索报告邮寄日期 17.2 月 2011 (17.02.2011)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		受权官员 吴卫民 电话号码: (86-10) 62411444

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/078611

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	无	
JP2000228668A	15.08.2000	无	

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



PCT



(10) 国际公布号

WO 2011/088700 A1

(43) 国际公布日
2011年7月28日 (28.07.2011)

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2010/078611
- (22) 国际申请日: 2010年11月10日 (10.11.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201010102646.2 2010年1月25日 (25.01.2010) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **张德智 (ZHANG, Dezhi)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **袁立权 (YUAN, Liquan)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

(54) 发明名称: 一种无源光网络系统组播业务加密方法和装置

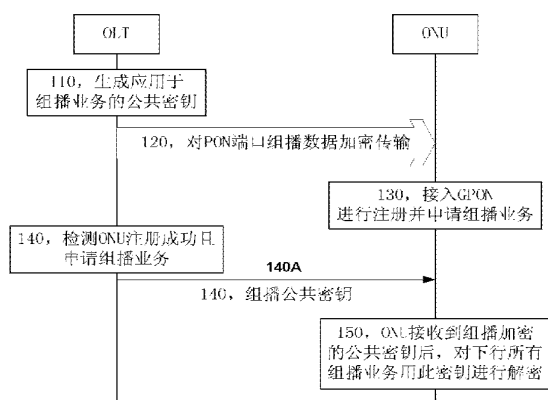


图1 / FIG. 1

(57) Abstract: A method for encrypting the multicast service in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generates a public key, transmits the multicast service data in a bearing channel after being encrypted using the public key, the multicast service data in the same bearing channel are encrypted using the same public key; and said OLT transmits the public key used to encrypt the multicast service data through a manage control channel to an Optical Network Unit (ONU) which has registered successfully and requested to receive said multicast service data. A device for encrypting the multicast service in a passive optical network system is also provided in the present invention. By applying the carrier channel encryption mechanism, the present invention is able to simplify the complexity of the OLT encryption mechanism and the ONU decryption mechanism, on the premise of ensuring the multicast service encryption.

[见续页]

- 110 GENERATING A PUBLIC KEY FOR THE MULTICAST SERVICE
120 ENCRYPTING AND TRANSMITTING THE MULTICAST DATA OF THE PON PORT
130 ACCESSING THE GPON, REGISTERING AND APPLYING THE MULTICAST SERVICE
140 DETECTING THE ONU HAVING REGISTERED SUCCESSFULLY AND HAVING APPLIED THE MULTICAST SERVICE
140A MULTICASTING THE PUBLIC KEY
150 AFTER RECEIVING THE PUBLIC KEY FOR ENCRYPTING THE MULTICAST, THE ONU DECRYPTS THE ENTIRE DOWNLINK MULTICAST SERVICE USING THE KEY



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种无源光网络系统组播业务加密方法,该方法包括:光线路终端(OLT)生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的组播业务数据使用相同的公共密钥加密;以及所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元(ONU)。本发明还公开了一种无源光网络系统组播业务加密装置。本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。

一种无源光网络系统组播业务加密方法和装置

技术领域

本发明涉及光通信领域，具体涉及一种用于无源光网络（Passive Optical Network, PON）系统中对组播业务数据进行加密的方法和装置。

背景技术

无源光网络的结构是一个 PON 口对应于多个 PON 终端用户光网络单元（Optical Network Unit, ONU）设备，且在下行链路上，每个用户 ONU 都能够接收局侧光线路终端（Optical Line Terminal, OLT）发出的所有数据。这里所说的“每个用户 ONU”包含合法用户和恶意用户两种情况：

拥有合法的注册信息，在物理连接到 PON 的某一根分支光纤后，可以和 OLT 交互消息进行注册，这种用户称之为合法用户；

不具有合法的注册信息，仅仅是在物理上连接到 PON 的某一根分支光纤，从不理会 OLT 发出的注册要求，仅接收下行信息，这种用户可以称之为恶意用户。

即使是合法用户，在其物理链接到一根分支光纤后，并在成功注册之前，也可以接收到 OLT PON 端口下发的各种明文数据包。目前 PON 技术中定义了一些加密机制，如吉比特无源光网络（Gigabit-Capable Passive Optical Network, GPON）系统的高级加密标准（Advanced Encryption Standard, AES）加密机制，或者以太网无源光网络（Ethernet Passive Optical Network, EPON）系统中的搅动加密机制和三重搅动加密机制等等，都是单播加密机制。对于组播数据（即 OLT PON 端口仅有一份业务数据下发，所有的用户或者符合要求的一部分用户接收并使用该业务数据），目前还没有有效的加密机制。一般运营商都是针对业务设置一个全网范围通用的密钥进行加密，但这种机制的缺点是一旦密钥被恶意用户得知，其全网所有业务内容都将被解密窃取。

运营商在 PON 中目前采用的方法是将组播业务数据包复制到每一个 PON 端口和用户 ONU 的单播通道上，应用单播机制进行加密，来保护组播

业务数据包不被恶意用户窃取。但是这种方法需要为每个 ONU 发送密钥，加重了 OLT 的负担。

发明内容

- 5 本发明要解决的技术问题是提供一种无源光网络系统组播业务加密方法和装置，提高安全性，简化 OLT 加密机制的复杂性，减轻 OLT 负荷。

为解决上述技术问题，本发明提供了一种无源光网络系统组播业务加密方法，该方法包括：

- 10 光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

所述方法还包括：

- 15 所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

所述方法还包括：

- 20 所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

- 25 OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请

接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

- 5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

为解决上述技术问题，本发明还提供了一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

- 10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

- 15 所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

- 25 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

本发明通过采用承载通道加密机制,可以在保证组播业务加密的前提下,简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制,可以将密码泄露后的影响范围从全网限制到某一个 PON 口,提高了组播业务内容的安全性。

- 5 另外,通过对无源光网络承载的组播业务数据进行加密后传输,以及仅将密钥发送给注册成功的用户,使得恶意用户无法获知上述密钥,且合法用户在注册之前也无法得到密钥,从而防止恶意用户窃取组播业务内容的非法行为,同时不会影响合法用户在注册后正常使用加密后的组播业务。

10 附图概述

此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

图 1 为本发明实施例一的流程图;

- 15 图 2 为本发明实施例二的流程图;

图 3 为本发明实施例三的流程;

图 4 为本发明实施例四的流程图。

本发明的较佳实施方式

- 20 本发明的发明构思是: OLT 生成公共密钥,并使用公共密钥对承载通道上的组播业务数据进行加密后发送,同一承载通道上的数据使用相同的公共密钥加密;所述 OLT 通过管理控制通道(例如光网络单元管理与控制接口(Optical Network Terminal (ONT) Management Control Interface, OMCI)或者操作管理维护(Operation Administration Maintenance, OAM))将加密
- 25 组播业务数据时所采用的公共密钥(简称公钥)发送给注册成功的且申请接收所述组播业务数据的 ONU。

ONU 获取公共密钥后,使用该密钥对承载通道上该 ONU 申请接收的组

播业务数据进行解密。

- 优选地，OLT 定期维护该公钥，可以在生成公共密钥的同时为公共密钥设置老化时间（如通过定时器设置），待老化时间到达后，重新生成公共密钥并使用新生成的公共密钥加密承载通道上的组播业务数据，向注册成功的
- 5 且申请接收所述组播业务数据的 ONU 发送新生成的公共密钥。多个公共密钥的老化时间可以相同也可以不同。或者 OLT 也可以在任何需要的时候，更新该公共密钥。

- 所述承载通道是 PON 的逻辑通道，可以是 GPON 端口承载的通用封装格式（General Encapsulation Model, GEM）通道，或 EPON 端口的逻辑链路标识（Logical Link Identification, LLID）通道，且由 OLT 进行维护更新。
- 10

所述管理控制通道也是 PON 的逻辑通道，例如可以是 GPON 系统的物理层操作管理维护（Physical Layer Operation Administration Maintenance, PLOAM）通道或 OMCI 通道，或者 EPON 系统中的扩展 OAM 通道。或者，采用数据通道发送公共密钥。

- 15 OLT 可同时生成多个公共密钥，分别用于对不同的承载通道进行数据加密。优选的，同一 PON 端口下的各条承载通道的公共密钥可以相同也可以不同，例如，可以设置每条承载通道有不同的公共密钥，也可以使部分承载通道使用相同的公共密钥。

- 20 当 OLT 对多条承载通道上的组播数据进行加密，且该多条承载通道可能发送给相同的 ONU 时，可在向 ONU 发送公共密钥的同时将使用该公共密钥进行组播业务数据加密的承载通道的承载通道标识一并发送给 ONU，即将承载所述组播业务数据的承载通道的承载通道标识发送给 ONU，以便 ONU 解密。但也不排除 ONU 通过逐一解密的方法找到使用该公共密钥的承载通道。

- 25 下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

本实施例为 GPON 系统传送公共密钥的实施例，应用范围是整个 GPON 物理端口，如图 1 所示，流程包括：

步骤 110，OLT 生成应用于组播业务的公共密钥；

步骤 120，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

5 步骤 130，ONU 上电，接入 GPON 向 OLT 发起注册并申请组播业务；

关于具体的注册过程以及申请组播业务的过程，GPON 协议已经有相关定义，本文不再赘述。

步骤 140，OLT 检测该 ONU 注册成功且申请组播业务，将生成的公共密钥发送给该 ONU；

10 ONU 是否注册成功以及 ONU 申请何种组播业务在 OLT 上均有记录。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

OLT 可以采用 GPON 协议中的 PLOAM 通道，或者 OMCI 通道或其他通道（如数据通道）将组播公共密钥传递给注册成功的 ONU。

15 步骤 150，ONU 接收到组播加密的公共密钥后，对下行所有组播业务应用此密钥进行解密。

实施例二

20 本实施例为 EPON 系统传送公共密钥且进行密钥更新的实施例，应用范围是整个 EPON 物理端口，如图 2 所示，流程包括：

步骤 210，OLT 生成应用于组播业务的公共密钥，并为该公共密钥设定一个定时器 T1；

该定时器用于控制公共密钥的老化时间。

步骤 220，OLT 对将在 PON 端口发送的组播数据进行加密后传输；

25 步骤 230，ONU 上电，接入 EPON 向 OLT 发起注册，并申请组播业务；

具体的注册过程以及申请组播业务的过程, EPON 协议已经有相关定义, 本文不再赘述。

步骤 240, ONU 请求 OLT 发送组播业务公共密钥;

步骤 250, OLT 接收到 ONU 的请求后, 查询该 ONU 如果处于注册成功
5 状态且该 ONU 申请组播业务, 则将生成的公共密钥发送给该 ONU;

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 260, ONU 接收到组播加密的公共密钥后, 对下行所有组播业务应用此密钥进行解密;

10 步骤 270, 当 T1 定时器超时, OLT 重新生成新的公共密钥, 并重置 T1 定时器 (以便下次 T1 超时后再次更新密钥)。

当有其他 ONU 请求 OLT 发送组播业务公共密钥时, OLT 将新生成的公共密钥发送给请求公共密钥的 ONU。并且, OLT 还需要为已经发送过公共密钥的 ONU 更新公共密钥。

15 OLT 可以采用 EPON 系统中的管理控制通道 (如扩展 OAM 通道) 或数据通道将生成的组播公共密钥传递给注册成功的 ONU。

实施例三

本实施例为 GPON 系统中非法用户试图接入业务被拒绝的示例, 应用范
20 围是整个 GPON 物理端口, 如图 3 所示, 流程包括:

步骤 310, OLT 生成应用于组播业务的公共密钥;

步骤 320, OLT 对将在 PON 端口发送的组播数据进行加密后传输;

步骤 330, 恶意用户 ONU 接入 GPON;

恶意用户接入 GPON 后可能不发起注册, 但如果发起注册的话必定无法
25 注册成功, 也无法申请组播业务。

步骤 340, 恶意用户 ONU 请求 OLT 发送组播业务公共密钥;

步骤 350, OLT 接收到请求后, 查询该 ONU 未能成功注册, 拒绝发送该组播公共密钥。

此时恶意 ONU 将无法获取组播公共密钥, 也就无法对组播业务内容进行解密, 运营商藉此防止了恶意用户的内容窃取。

实施例四

本实施例为 GPON 系统传送公共密钥的实施例, 应用范围是 GPON 物理端口中对应某一组播业务的一个 GEM 通道, 本实施例中的 ONU 仅申请了第一 GEM 通道上的组播业务, 如图 4 所示, 流程包括:

步骤 410, OLT 生成应用于第一 GEM 通道的组播公共密钥 A, 以及应用于第二 GEM 通道的组播公共密钥 B;

步骤 420, OLT 将承载在第一 GEM 通道的组播业务数据用公共密钥 A 加密后传输, 该通道所有 ONU 共享此公共密钥 A;

步骤 430, OLT 将承载在第二 GEM 通道的组播业务数据用公共密钥 B 加密后传输, 该通道所有 ONU 共享此公共密钥 B;

上述步骤 420 和 430 的执行顺序不固定。

步骤 440, ONU 上电, 接入 GPON 向 OLT 发起注册并申请组播业务;

步骤 450, OLT 检测到该 ONU 注册成功且申请接收的是第一 GEM 通道上的组播业务, 将该公共密钥 A 和对应的第一 GEM 通道标识传送给该 ONU;

在其他实施例中, 也可以由 ONU 主动发起密钥请求。

OLT 根据自身策略可以在检测到 ONU 申请组播业务成功后向 ONU 发送公共密钥或只要检测到 ONU 申请组播业务就向 ONU 发送公共密钥。

步骤 460, ONU 接收到公共密钥 A 和对应的第一 GEM 通道标识后, 对第一 GEM 通道中传输的组播业务数据进行解密。

ONU1 未接收到公钥 B，无法解密下行第二 GEM 通道数据。可见，当同一 ONU 接收多个组播业务且该多个组播业务数据承载在不同的承载通道上时，OLT 需要在发送公钥的同时将该公钥对应的承载通道标识发送给该 ONU。

- 5 OLT 可以采用 GPON 协议中的 PLOAM 通道维护通道，或者 OMCI 管理通道或其他通道将组播公共密钥传递给注册成功的 ONU。

一个公共密钥可以用于一条 GEM 通道，也可以用于多条，即多条 GEM 通道共用一个密钥。

- 10 实现上述方法的 OLT 包括密钥生成单元、加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

- 15 所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU。

优选地，所述装置还包括：

老化时间设置单元，其设置为：对密钥生成单元生成的公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

- 20 所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

- 25 所述发送单元还设置为：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用5 硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围10 之内。

工业实用性

本发明通过采用承载通道加密机制，可以在保证组播业务加密的前提下，15 简化 OLT 加密机制以及 ONU 解密机制复杂度。相比于现有的组播业务加密机制，可以将密码泄露后的影响范围从全网限制到某一个 PON 口，提高了组播业务内容的安全性。

另外，通过对无源光网络承载的组播业务数据进行加密后传输，以及仅将密钥发送给注册成功的用户，使得恶意用户无法获知上述密钥，且合法用20 户在注册之前也无法得到密钥，从而防止恶意用户窃取组播业务内容的非法行为，同时不会影响合法用户在注册后正常使用加密后的组播业务。

权 利 要 求 书

1、一种无源光网络系统组播业务加密方法，该方法包括

光线路终端（OLT）生成公共密钥，并使用公共密钥对承载通道上的组播业务数据进行加密后发送，同一承载通道上的组播业务数据使用相同的公共密钥加密；以及

所述 OLT 通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

2、如权利要求 1 所述的方法，其还包括：

所述 ONU 获取公共密钥后，使用所述公共密钥对承载通道上所述 ONU 申请接收的组播业务数据进行解密。

3、如权利要求 1 或 2 所述的方法，其还包括：

所述 OLT 在生成公共密钥的同时为公共密钥设置老化时间，待老化时间到达后，重新生成新的公共密钥，并使用新的公共密钥加密承载通道上的组播业务数据，向注册成功的且申请所述组播业务数据的 ONU 发送所述新的公共密钥。

4、如权利要求 1 所述的方法，其中：

所述 OLT 将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU 的步骤包括：

OLT 判断 ONU 注册成功且申请接收组播业务数据，则主动将加密所述组播业务数据时所采用的公共密钥发送给所述 ONU；或者

所述 ONU 向 OLT 请求密钥，所述 OLT 检测所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据所采用的公共密钥发送给所述 ONU。

5、如权利要求 1 所述的方法，其中：

不同承载通道上的组播业务数据使用的公共密钥相同或不同。

6、如权利要求 1 或 2 所述的方法，其中：

5 所述 OLT 在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的步骤中，所述 OLT 还向所述 ONU 发送使用所述公共密钥进行组播业务数据加密的承载通道的承载通道标识。

7、一种无源光网络系统组播业务加密装置，该装置包括密钥生成单元，加密单元以及发送单元，其中：

所述密钥生成单元设置为：生成公共密钥；

10 所述加密单元设置为：对承载在同一承载通道上的组播业务数据使用相同的公共密钥进行加密；

所述发送单元设置为：发送加密后的组播业务数据，以及通过管理控制通道将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的光网络单元（ONU）。

15 8、如权利要求 7 所述的装置，其中，

所述装置还包括老化时间设置单元，所述老化时间设置单元设置为：为公共密钥设置老化时间，当老化时间到达时，通知所述密钥生成单元重新生成公共密钥。

9、如权利要求 7 所述的装置，其中：

20 所述发送单元是设置为按如下方式将加密组播业务数据时所采用的公共密钥发送给注册成功的且申请接收所述组播业务数据的 ONU：判断 ONU 注册成功且申请接收组播业务数据后，主动将加密所述组播业务数据时采用的公共密钥发送给所述 ONU；或者，在接收到 ONU 请求密钥的请求后，判断所述 ONU 注册成功且申请接收组播业务数据，则将加密所述组播业务数据

所采用的公共密钥发送给所述 ONU。

10、如权利要求 7 或 9 所述的装置，其中，

所述发送单元还设置为：在向注册成功的且申请接收所述组播业务数据的 ONU 发送公共密钥的同时，还向所述 ONU 发送使用所述公共密钥进行组
5 播业务数据加密的承载通道的承载通道标识。

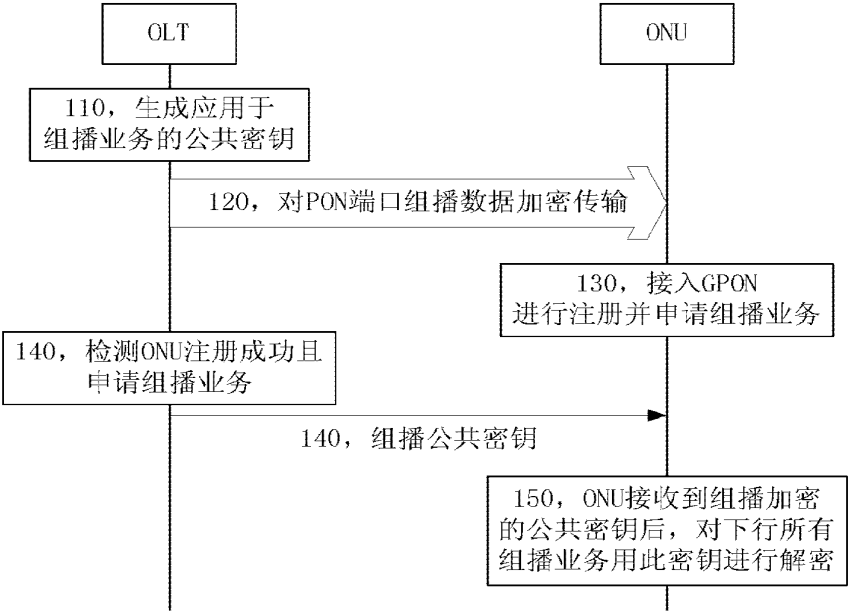


图 1

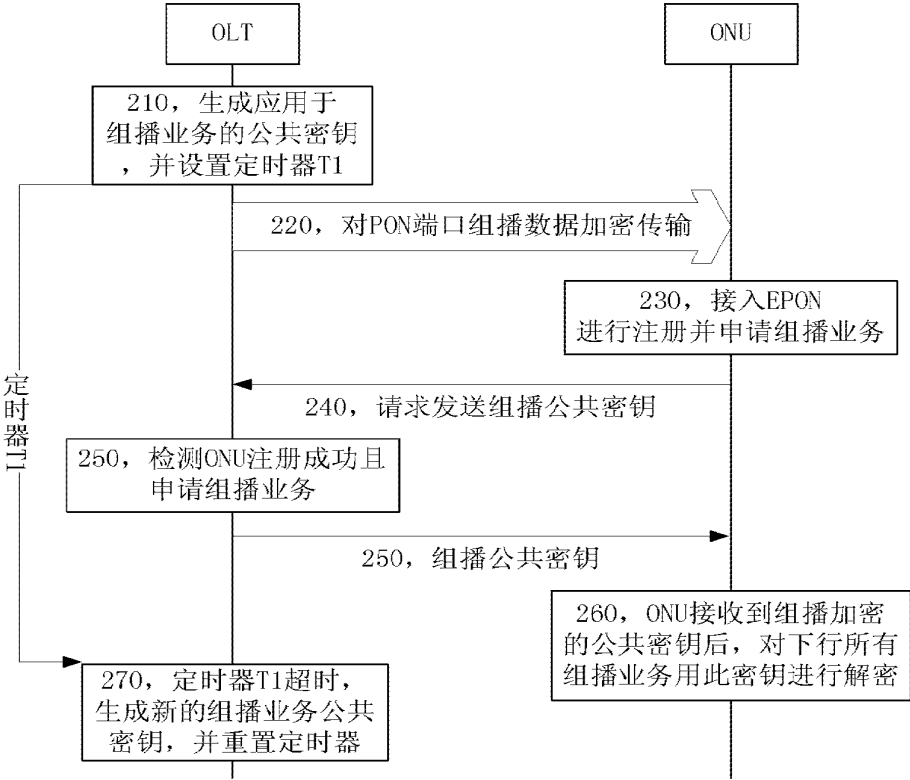


图 2

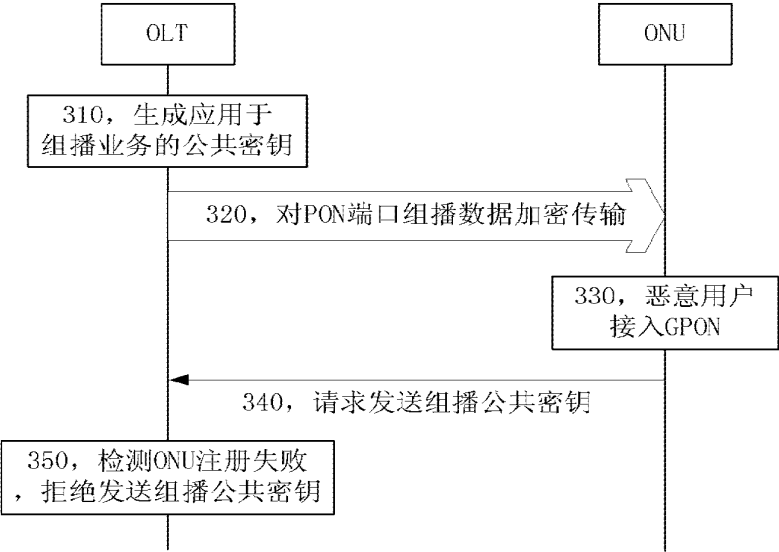


图 3

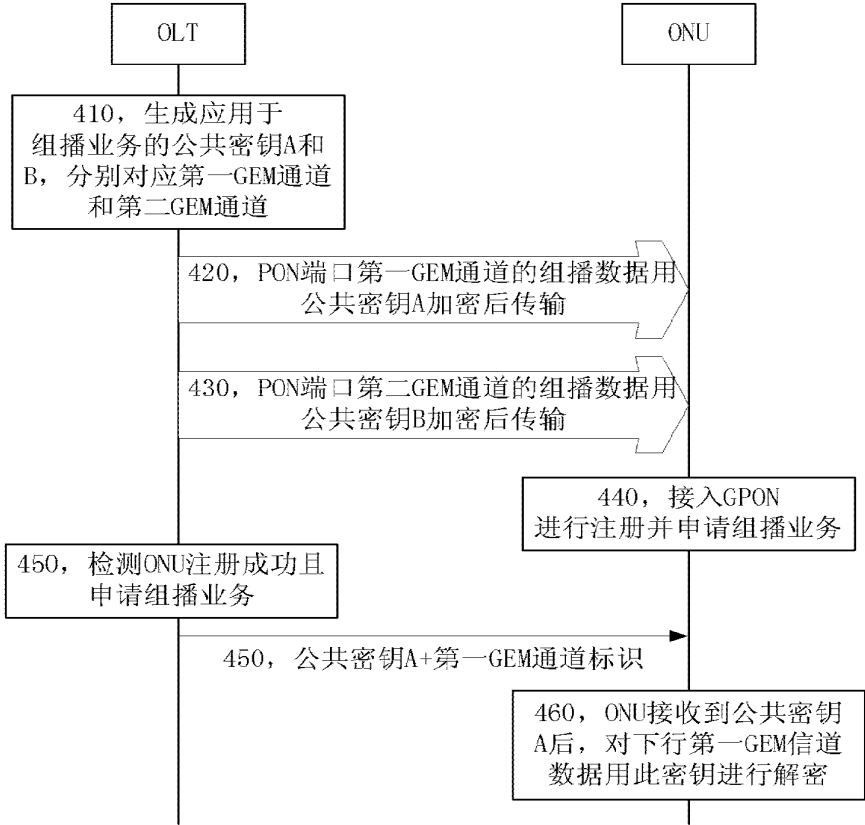


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/078611

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, H04J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CPRS, CPRSABS, WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1866857A (HUAWEI TECHNOLOGIES CO., LTD) 22 Nov. 2006(22.11.2006) Description pages 2, 5-6, Figs. 2-3	1-10
X	CN1855834A (HUAWEI TECHNOLOGIES CO., LTD) 01 Nov. 2006(01.11.2006) Description pages 4-5, Fig. 4	1-10
A	JP2000228668A (NEC CORP) 15 Aug. 2000(15.08.2000) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
21 Jan. 2011(21.01.2011)

Date of mailing of the international search report
17 Feb. 2011 (17.02.2011)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
WU, Weimin
Telephone No. (86-10)62411444

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/078611

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	NONE	
JP2000228668A	15.08.2000	NONE	

Form PCT/ISA /210 (patent family annex) (July 2009)

国际检索报告

 国际申请号
PCT/CN2010/078611

A. 主题的分类		
H04L 9/00 (2006.01) i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L, H04W, H04J		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNKI, CPRS, CPRSABS: 光网络, PON, EPON, GPON, OLT, ONU, ONT, 加密, 解密, 密钥, 公钥, 组播, 多播 WPI, EPODOC, DWPI, SIPOABS: optical w network, PON, EPON, GPON, OLT, ONU, ONT, encrypt+, cipher+, decrypt+, key, public w key, multicast+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN1866857A (华为技术有限公司) 22.11 月 2006(22.11.2006) 说明书 2, 5-6 页, 图 2-3	1-10
X	CN1855834A (华为技术有限公司) 01.11 月 2006(01.11.2006) 说明书 4-5 页, 图 4	1-10
A	JP2000228668A (NEC CORP) 15.8 月 2000(15.08.2000) 全文	1-10
☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件		“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件
国际检索实际完成的日期 21.1 月 2011(21.01.2011)		国际检索报告邮寄日期 17.2 月 2011 (17.02.2011)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 吴卫民 电话号码: (86-10) 62411444

PCT/ISA/210 表(第 2 页) (2009 年 7 月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/078611

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1866857A	22.11.2006	WO2007033553A1	29.03.2007
CN1855834A	01.11.2006	无	
JP2000228668A	15.08.2000	无	

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/22 (2006.01)

H04L 9/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510034337.5

[43] 公开日 2006 年 11 月 1 日

[11] 公开号 CN 1855834A

[22] 申请日 2005.4.20

[21] 申请号 200510034337.5

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 江 涛 何 纲 赵 峻 吴文胜

[74] 专利代理机构 中原信达知识产权代理有限责任
公司

代理人 王永文

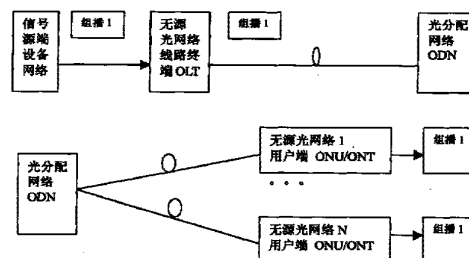
权利要求书 2 页 说明书 6 页 附图 4 页

[54] 发明名称

一种实现无源光网络组播的方法

[57] 摘要

一种实现 PON 组播的方法，对于具有组播接收权限的多个光网络用户端，光网络线路终端对于同一个组播，分配一个下行业务通道，只发送一份组播数据流；光网络线路终端向具有组播接收权限的光网络用户端开通所述下行业务通道的权限，使该光网络用户端能接收该组播数据流。可以由光网络线路终端产生一个密钥，并把该密钥作为该组播的公共密钥，在发送组播数据流时，利用该密钥进行加密；并将该密钥利用另一业务通道发送给具有组播接收权限的光网络用户端，光网络用户端利用该密钥对组播数据流进行解密，接收该组播数据流。利用本发明，只需要发送一份组播数据流即可实现 PON 组播，节省了下行数据带宽。



1、一种实现无源光网络组播的方法，其特征在于：

对于具有组播接收权限的多个光网络用户端，光网络线路终端对于同一个组播，分配一个下行业务通道，只发送一份组播数据流；

5 光网络线路终端向具有组播接收权限的光网络用户端开通所述下行业务通道的权限，使该光网络用户端能接收该组播数据流。

2、根据权利要求 1 所述的实现无源光网络组播的方法，其特征在于：由光网络线路终端产生一个密钥，并把该密钥作为该组播的公共密钥，在发送组播数据流时，利用该密钥进行加密；并将该密钥利用另一
10 业务通道发送给具有组播接收权限的光网络用户端，光网络用户端利用该密钥对组播数据流进行解密，接收该组播数据流。

3、根据权利要求 1 或 2 所述的实现无源光网络组播的方法，其特征在于：先由光网络用户端向光网络线路终端发送组播申请，光网络线路终端对组播申请进行处理，再根据用户权限决定是否向该光网络用户
15 端分配组播。

4、根据权利要求 3 所述的实现无源光网络组播的方法，其特征在于：如果用户没有组播权限，光网络线路终端不对该组播申请进行处理；如果用户有组播权限且还不存在该组播时，则处理过程如下：

A1、光网络线路终端向上申请获得新的数据组播；

20 A2、光网络线路终端分配该组播占用一个下行业务通道；

A3、由光网络线路终端产生一个密钥，并把该密钥作为该组播的公共密钥；

A4、光网络线路终端使用另一业务通道把该密钥发送给相应的光网

络用户端;

A5、光网络线路终端利用所分配的下行业务通道作为组播数据传输通道,向有权限的光网络用户端开通该下行业务通道的权限;

A6、光网络线路终端根据密钥对组播数据流加密后发送,有权限的
5 光网络用户端根据该密钥接收组播数据流。

5、根据权利要求 4 所述的实现无源光网络组播的方法,其特征在于:如果用户有组播权限,且已经存在该组播时,则处理过程如下:

B1、光网络线路终端使用另一业务通道把该组播的公共密钥发送给该光网络用户端;

10 B2、光网络线路终端向该光网络用户端开通下行业务通道的权限;

B3、光网络用户端根据组播公共密钥接收加密组播数据流。

6、根据权利要求 3 所述的实现无源光网络组播的方法,其特征在于:光网络用户端要退出组播时,由光网络用户端向光网络线路终端发送离开组播申请,光网络线路终端处理离开组播组申请,关闭该用户该
15 组播的下行业务通道权限。

7、根据权利要求 6 所述的实现无源光网络组播的方法,其特征在于:如果是最后一个组播用户,则光网络线路终端向上级网络发送离开组播申请,光网络线路终端停止从上级网络接收该组播流,关闭该组播通道的使用。

20 8、根据权利要求 3 所述的实现无源光网络组播的方法,其特征在于:所述的业务通道由通道号、虚拟信道标识符或虚拟通路标识符标识。

9、根据权利要求 3 所述的实现无源光网络组播的方法,其特征在于:所述的光网络用户端为光网络用户单元或光网络用户终端。

一种实现无源光网络组播的方法

技术领域

本发明涉及无源光网络（PON）技术领域，尤其涉及一种实现无源
5 光网络组播的方法。

背景技术

近年来，随着互联网的快速发展和个人电脑的普及，Internet 数据流的激增加剧了接入部分的容量限制，接入网中传统的铜缆接入方式显然
10 已经无法满足通信业务增长的需求。由于光纤具有传输频带宽、容量大、损耗低、抗干扰能力强等优点，非常适合作为高速、宽带业务的传输媒体。而在各种光接入技术中，PON（无源光网络）由于采用无源节点、敷设和运行维护成本低、对业务透明和易于升级等优点而备受关注。

PON（无源光网络）是现在和未来光接入非常有前途的技术，作为
15 一种新兴的覆盖最后一公里的宽带接入光纤技术，其在光分支点不需要节点设备，只需安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。同时，数字多媒体信号也越来越受到人们的青睐，通过接入网络实现视频或音频的点播、组播和广播等应用，将更多地出现在
20 目前和以后的网络接入系统中。

如图 1 所示为 PON 组播网络结构示意图，无源光网络从光网络线路终端（OLT）接入信号，通过光分配网络（ODN）分配给各用户端（ONU/ONT，ONT 为光网络用户终端，直接位于用户端；而 ONU 为光网络用户单元，与用户间还有其它的网络如以太网），在用户端可收看多媒体

信号。其中 OLT 位于局端，ONU/ONT 位于用户端，OLT 到 ONU/ONT 的方向为下行方向，反之为上行方向。下行方向采用基于时分复用的组播方式，由 ODN 将由 OLT 输入的光信号按功率平均分配到若干输出用户端，一般有 1 分 16、1 分 32 或 1 分 64 等分配方案。

- 5 如图 2 所示为现有技术 OLT 组播包复制原理示意图，组播方法是，在 OLT 局端处理组播时，将组播包复制成多个组播包，加入了组播的用户端 ONU/ONT 分别接收相应的组播复制包。

10 现有技术的缺点在于每个组播频道有多个用户申请时，OLT 将复制成多个数据包，分时向 ONU/ONT 传送，各 ONU/ONT 获取相应的数据包，因此，将占用较多的下行数据带宽。例如：有 10 个组播频道，平均有 10 个用户申请，设数据流为 5Mbit/s 时，则下行带宽将占用带宽为： $10 \times 10 \times 5 = 500\text{Mbit/s}$ 。

发明内容

- 15 本发明所要解决的技术问题是：克服现有技术无源光网络组播时占用较多下行数据带宽的不足，提供一种实现无源光网络组播的方法，减小组播下行传输中对频带的占用带宽。

本发明为解决上述技术问题所采用的技术方案为：

- 20 这种实现无源光网络组播的方法，对于具有组播接收权限的多个光网络用户端，光网络线路终端对于同一个组播，分配一个下行业务通道，只发送一份组播数据流；光网络线路终端向具有组播接收权限的光网络用户端开通所述下行业务通道的权限，使该光网络用户端能接收该组播数据流。

- 25 可以由光网络线路终端产生一个密钥，并把该密钥作为该组播的公共密钥，在发送组播数据流时，利用该密钥进行加密；并将该密钥利用另一业务通道发送给具有组播接收权限的光网络用户端，光网络用户端

利用该密钥对组播数据流进行解密，接收该组播数据流。

可以先由光网络用户端向光网络线路终端发送组播申请，光网络线路终端对组播申请进行处理，再根据用户权限决定是否向该光网络用户端分配组播。如果用户没有组播权限，光网络线路终端不对该组播申请
5 进行处理；如果用户有组播权限，且还不存在该组播时，则处理过程如下：

A1、光网络线路终端向上申请获得新的数据组播；

A2、光网络线路终端分配该组播占用一个下行业务通道；

A3、由光网络线路终端产生一个密钥，并把该密钥作为该组播的公
10 共密钥；

A4、光网络线路终端使用另一业务通道把该密钥发送给相应的光网络用户端；

A5、光网络线路终端利用所分配的下行业务通道作为组播数据传输通道，向有权限的光网络用户端开通该下行业务通道的权限；

15 A6、光网络线路终端根据密钥对组播数据流加密后发送，有权限的光网络用户端根据该密钥接收组播数据流。

如果用户有组播权限，且已经存在该组播时，则处理过程如下：

B1、光网络线路终端使用另一业务通道把该组播的公共密钥发送给该光网络用户端；

20 B2、光网络线路终端向该光网络用户端开通下行业务通道的权限；

B3、光网络用户端根据组播公共密钥接收加密组播数据流。

光网络用户端要退出组播时，由光网络用户端向光网络线路终端发送离开组播申请，光网络线路终端处理离开组播组申请，关闭该用户该组播的下行业务通道权限。如果是最后一个组播用户，则光网络线路终端
25 向上级网络发送离开组播申请，光网络线路终端停止从上级网络接收该组播流，关闭该组播通道的使用。

所述的业务通道可以采用通道号、虚拟信道标识符或虚拟通路标识符标识。所述的光网络用户端可为光网络用户单元或光网络用户终端。

本发明的有益效果为：利用本发明，只需要发送一份组播数据流即可实现 PON 组播，节省了下行数据带宽。OLT 可以给下行组播用户提供更好的带宽能力，每个组播频道无论有多少个用户申请，都不会影响下行的传输数据带宽，因此系统能提供更多组播频道给用户同时使用。可以对组播数据流进行加密，并将密钥发送给用户端，用户端根据密钥进行解密，这样进一步确保了组播数据的安全性，确保有组播权限的用户才能接收到组播数据。

10

附图说明

图 1 为 PON 组播网络结构示意图；

图 2 为现有技术 OLT 组播包复制原理示意图；

图 3 为本发明 OLT 组播实现原理示意图；

15

图 4 为本发明组播申请流程图；

图 5 为本发明组播退出流程图。

具体实施方式

下面根据附图和实施例对本发明作进一步详细说明：

20 如图 3 所示，本发明提供一种实现无源光网络组播的方法，将组播代理放在光网络线路终端（OLT）内，即各用户端（如 ONU/ONT）的组播申请向 OLT 发送，OLT 处理组播申请，向 ONU/ONT 发送组播数据流。多个 ONU/ONT 申请同一个组播数据流时，OLT 利用一个业务通道只发送一份组播数据流，申请该组播的 ONU/ONT 均获得该组播数据流
25 的接收权限，从而实现组播功能。

可以由 OLT 产生一个密钥，并把该密钥作为该组播的公共密钥，在

发送组播数据流时，利用该密钥进行加密；并将该密钥利用另一业务通道发送给具有组播接收权限的光网络用户端，光网络用户端利用该密钥对组播数据流进行解密，接收该组播数据流，这样确保有组播权限的用户才能接收到组播数据。

5 如图 4 所示为本发明组播申请流程图，组播申请步骤如下：

1、由用户端（以 ONU 为例进行说明）向 OLT 发送 IGMP（互联网组管理协议）包申请组播；

2、OLT 处理组播申请，根据用户权限，决定是否分配组播；

3、如果用户没有组播权限，则 OLT 不再对该组播申请进行处理；

10 如果用户有组播权限，则 OLT 处理组播；

4、OLT 处理组播时，如果还不存在该组播，则处理过程如下：

1) OLT 向上申请获得新的数据组播，产生一个组播地址和组播流；

2) OLT 分配该组播占用一个下行业务通道（可由通道号 Port-ID、虚拟通路标识符 VPI 或虚拟信道标识符地址 VCI 来标识，Port-ID 为 GPON 数据帧子结构 GEM 帧的一个字段，为 PON 中的多路复用业务提供业务标识；VPI/VCI 为 GPON 数据帧子结构 ATM 帧中的字段）；

15

3) 由 OLT 产生一个密钥，OLT 把该密钥作为该组播的公共密钥；

4) OLT 使用另一业务通道（可由通道号 Port-ID、虚拟通路标识符 VPI、虚拟信道标识符地址 VCI 来标识）把该密钥发送给相应的 ONU 用户；

20

5) OLT 利用所分配的下行业务通道作为组播数据传输通道，向有权限的组播用户开通该下行业务通道的权限；

6) OLT 利用所述密钥对组播数据流进行加密并发送，ONU 根据所接收到的密钥进行解密，从而获得组播数据。

25 如果已经存在该组播，则处理步骤如下：

1) OLT 向该用户开通另一特定业务通道的权限，并使用特定业务

通道把该组播的公共密钥发送给该 ONU 用户；

2) OLT 向该用户开通组播下行业务通道的权限；

3) ONU 根据所接收到的密钥进行解密，从而获得组播数据。

如图 5 所示为本发明组播退出流程图，步骤如下：

5 1、ONU 向 OLT 发送 IGMP 离开组播组申请；

2、OLT 处理离开组播申请，关闭该用户该组播的业务通道权限；

3、如果不是最后一个组播用户，则 OLT 不进行任何额外处理，等待其它组播信息命令处理；

如果是最后一个组播用户，则 OLT 向上级网络发送 IGMP 离开组播
10 组申请，OLT 停止从上级网络接收该组播流，关闭组播通道的使用，等待其它组播信息命令处理。

当然，OLT 也可以不产生密钥，可以由 OLT 直接向 ONU/ONT 发送组播数据流。即，OLT 利用一个业务通道发送一份组播数据流，由 OLT 通过管理通道或其他通道给 ONU 分配组播接收权限，只有具有接收权
15 限的 ONU/ONT 才可以获得该组播数据流。同样这种不加密方法，也只需要发送一份组播数据流即可实现 PON 组播。

利用本发明，使用相同业务通道（如相同 Port-ID 或 VPI/VCI 的业务通道）给同一组播用户传输组播加密数据流，使用不同业务通道分别给同一组播的不同用户传输组播加密密钥。这样使在 PON 网络的接入
20 系统中，减小了传统组播下行传输中对频带的占用带宽，OLT 可以给下行组播用户提供更好的带宽能力，每个组播频道无论有多少个用户申请，都不会影响下行的传输数据带宽，系统能提供更多组播频道给用户同时使用。本领域技术人员不脱离本发明的实质和精神，可以有多种变形方案实现本发明，以上所述仅为本发明较佳可行的实施例而已，并非
25 因此局限本发明的权利范围，凡运用本发明说明书及附图内容所作的等效结构变化，均包含于本发明的权利范围之内。

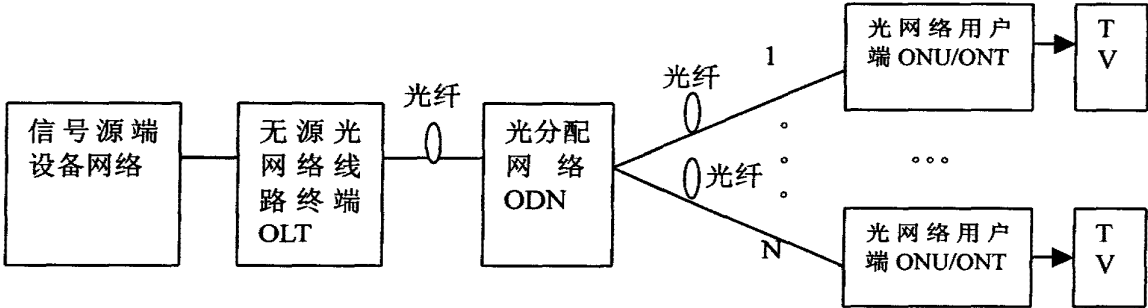


图1

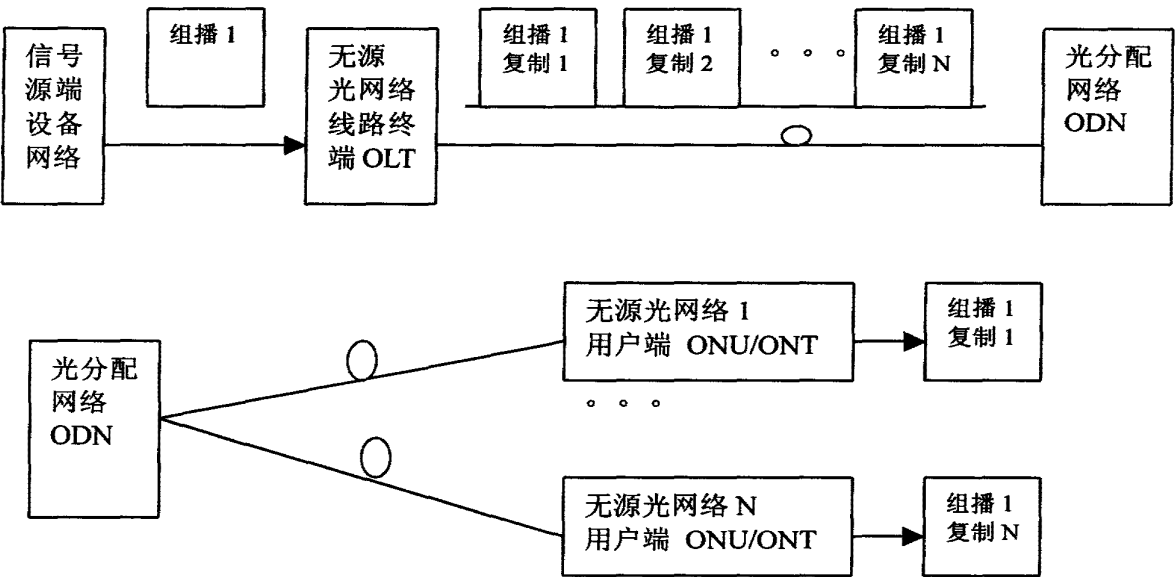


图2

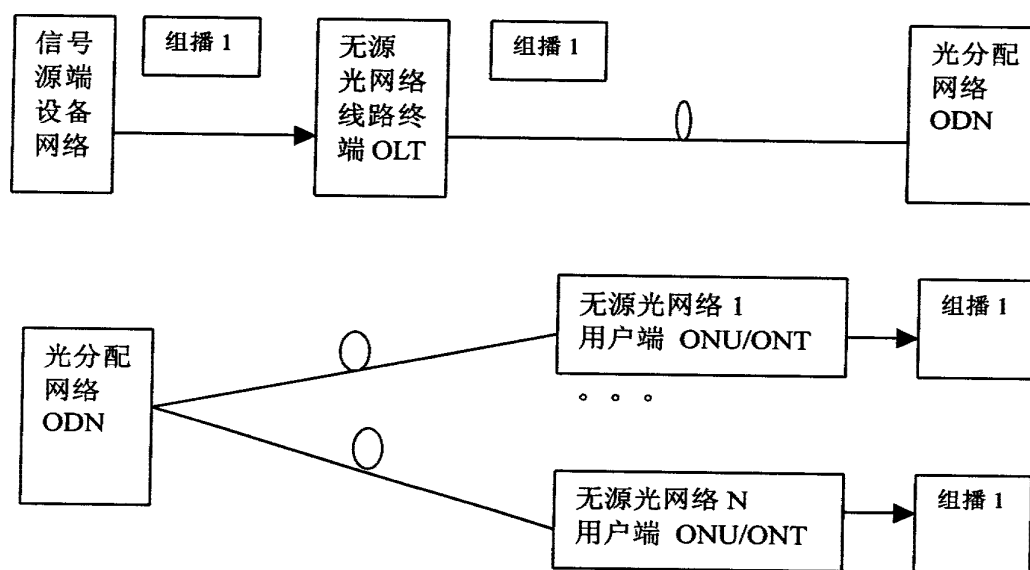


图 3

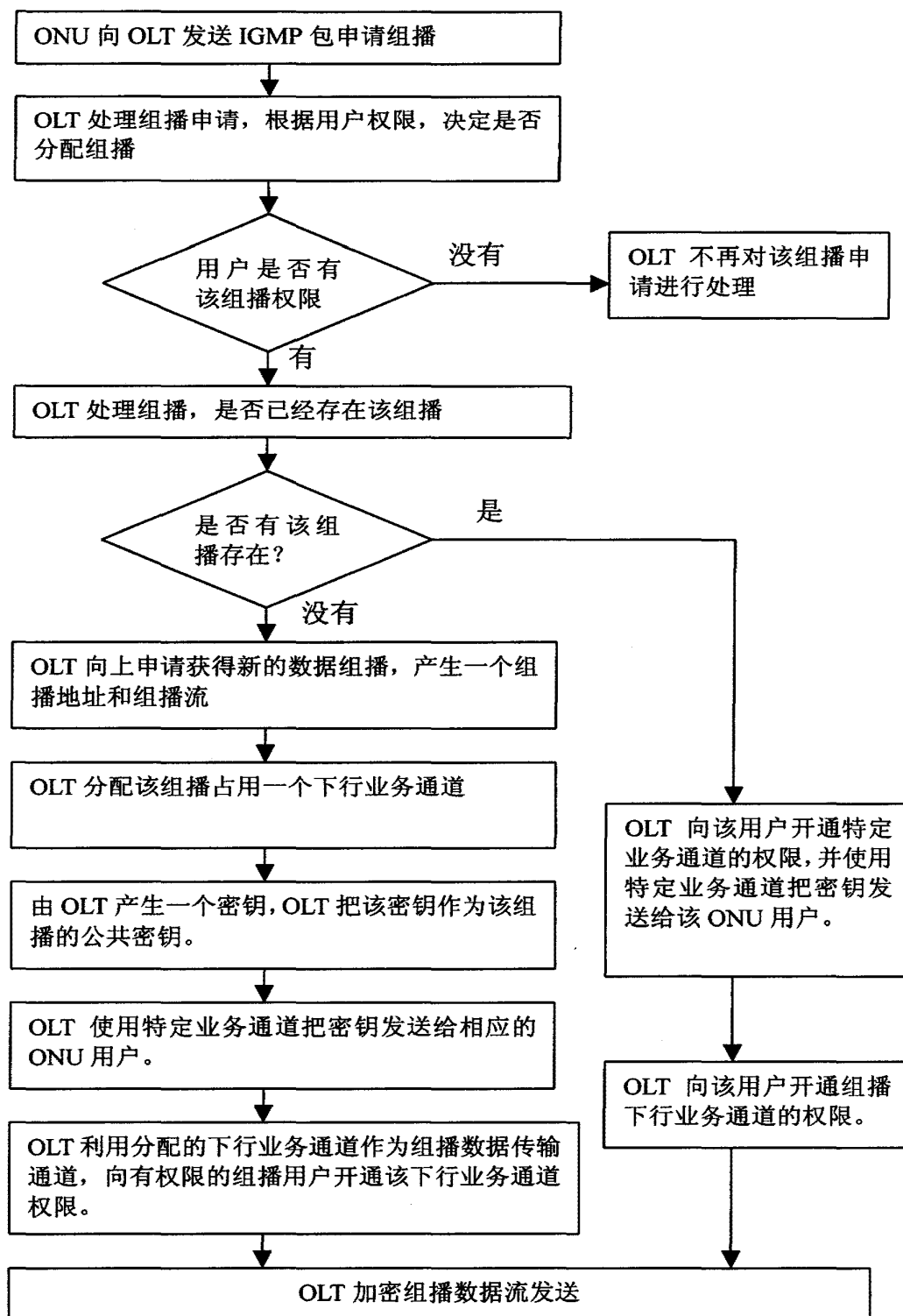


图4

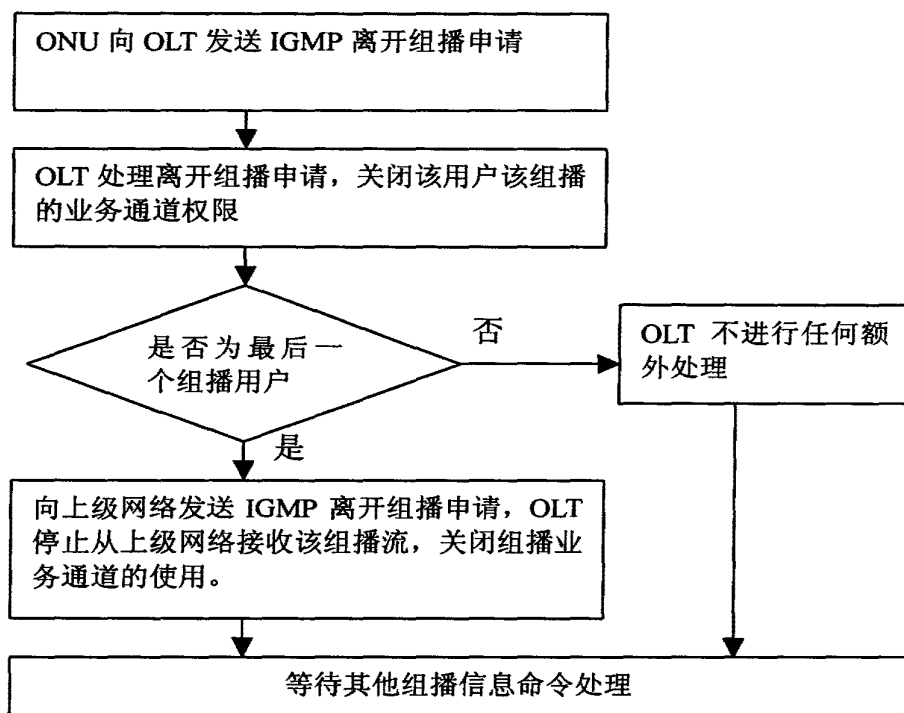


图5

What is claimed is:

1. A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a public key, and using the public key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same public key to carry out encryption; and

said OLT sending the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

2. The method of claim 1, further comprising:

after obtaining the public key, said ONU using said public key to decrypt the multicast service data, which the ONU applies to receive, in the bearer channel.

3. The method of claim 1 or 2, further comprising:

said OLT generating the public key and setting an aging time for the public key, and after the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data.

4. The method of claim 1, wherein:

the step of said OLT sending the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the public key applied in encrypting the multicast service data to said ONU; or

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the public key applied in encrypting said multicast service data to the ONU.

5. The method of claim 1, wherein:

the multicast service data in different bearer channels use different public keys or the same public key.

6. The method of claim 1 or 2, wherein:

in the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

7. A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a public key;

said encryption unit is configured to: encrypt multicast service data born in a same one bearer channel with a same public key;

said sending unit is configured to: send the encrypted multicast service data, and send the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

8. The device of claim 7, wherein,

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the public key, and when the aging time arrives, notifying said key generation unit to regenerate a public key.

9. The device of claim 7, wherein:

said sending unit is configured to apply following methods to send the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the public key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast

service data, and then sending the public key applied in encrypting the multicast service data to the ONU.

10. The device of claim 7 or 9, wherein,

said sending unit is also configured to: send the public key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

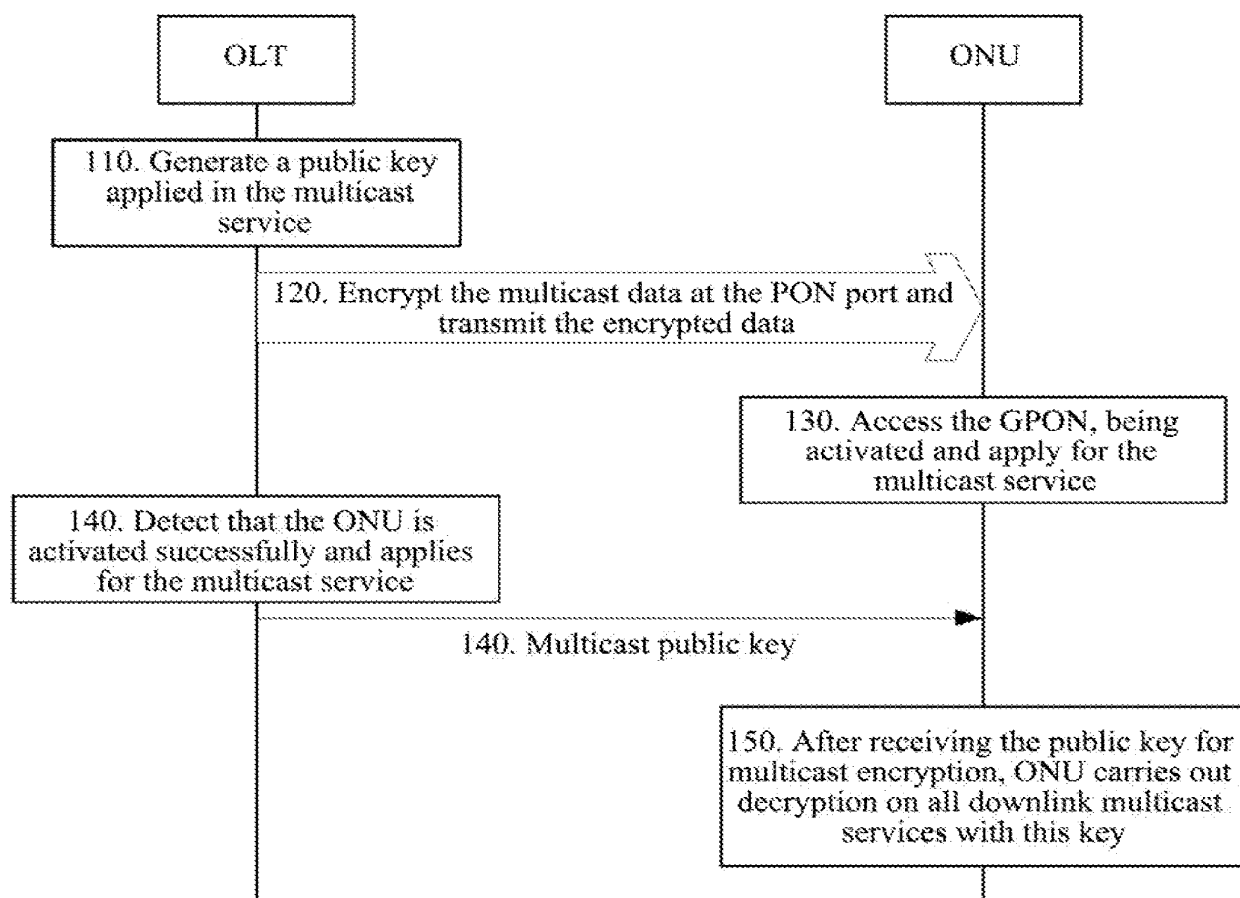


FIG. 1

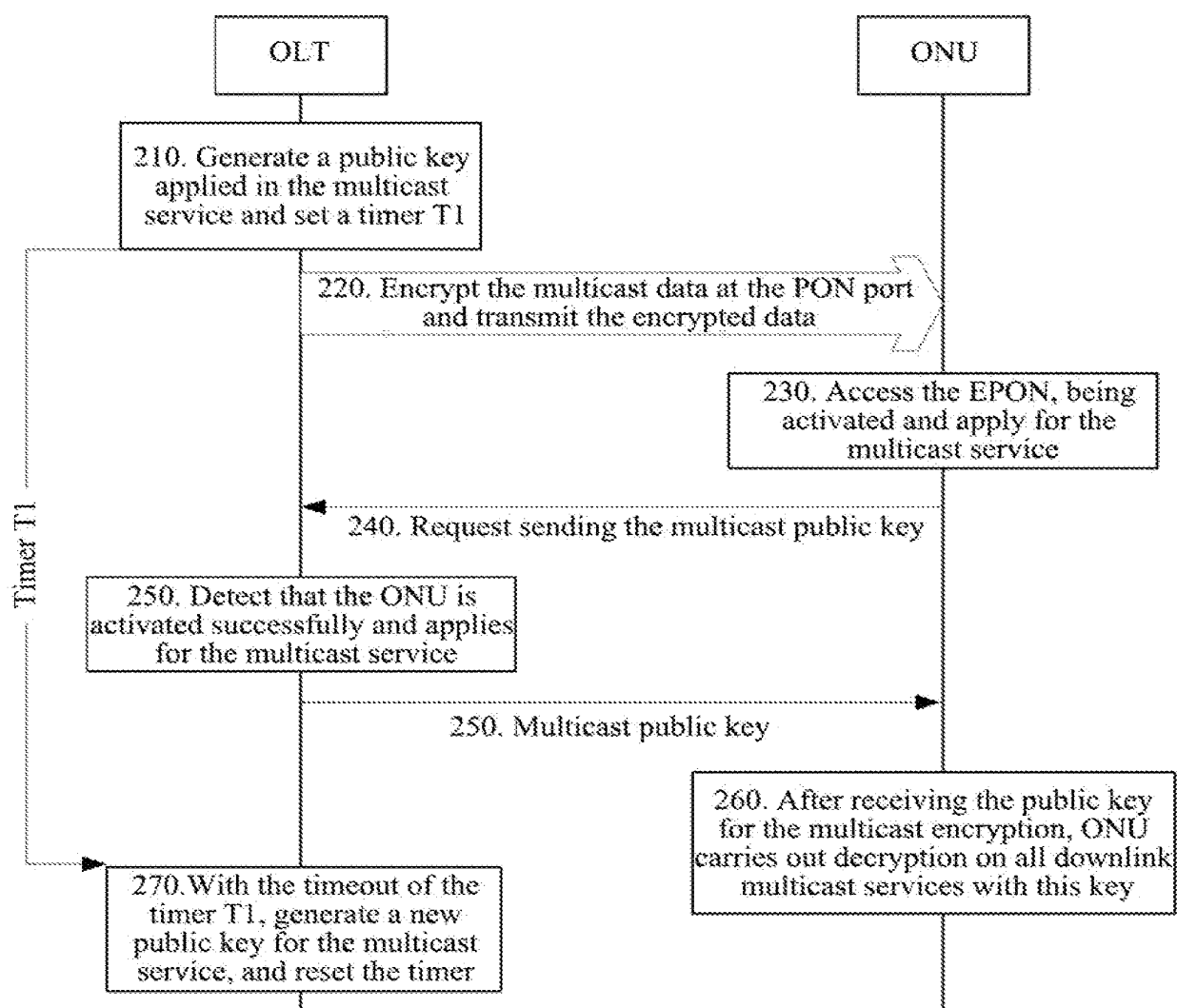


FIG. 2

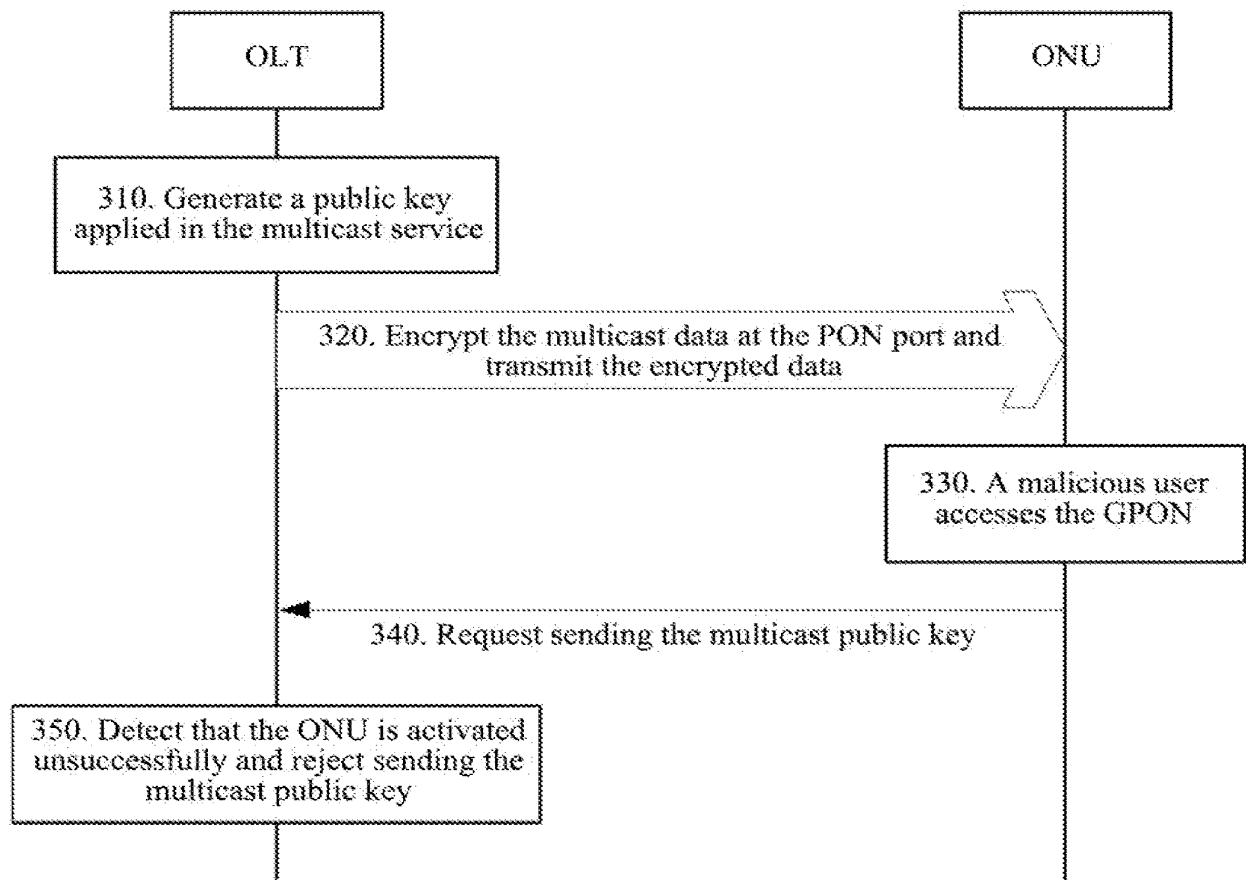


FIG. 3

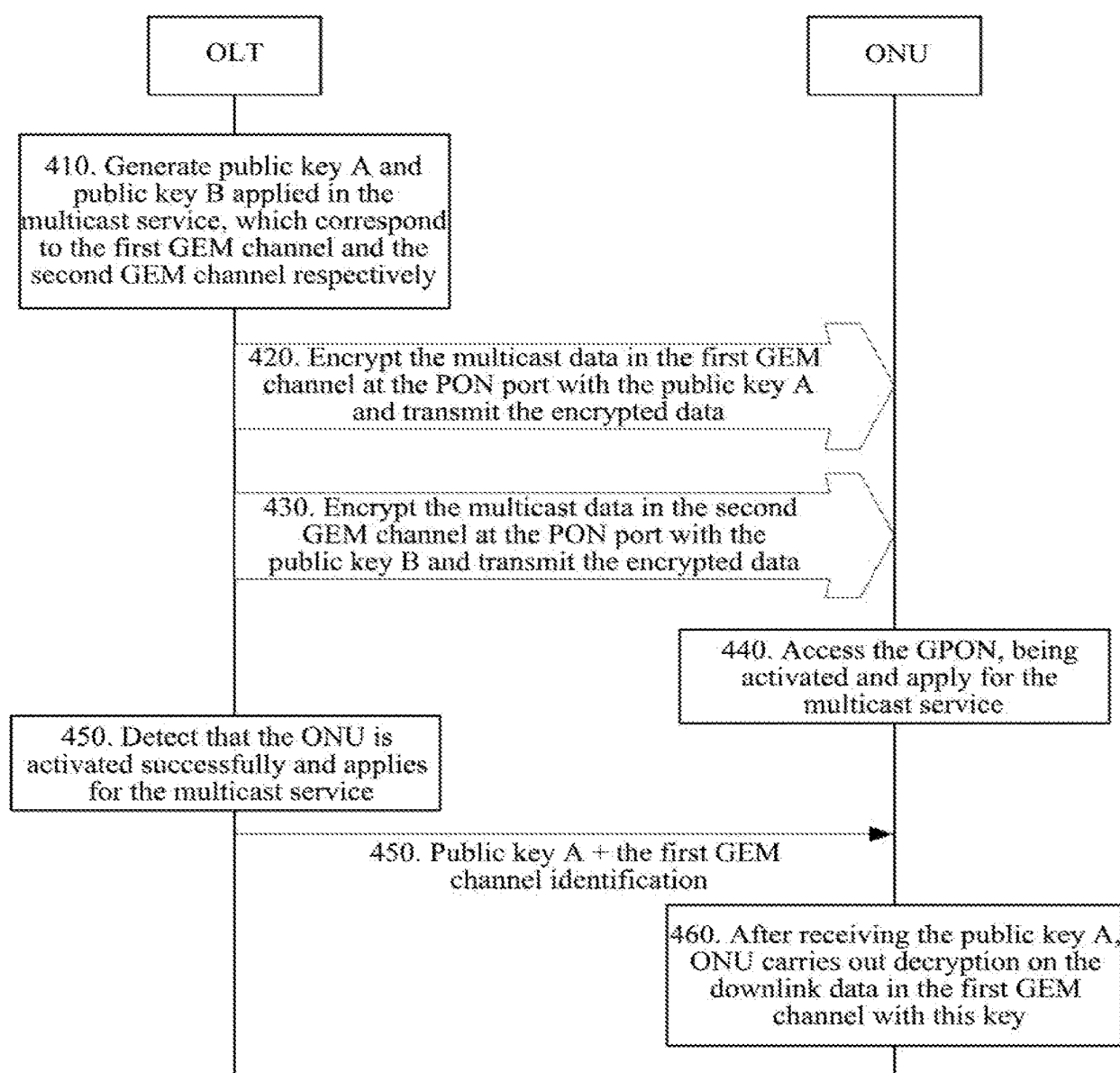


FIG. 4

JOINT DECLARATION FOR PATENT APPLICATION (37 CFR 1.63) AND POWER OF ATTORNEY

As the below named inventors, we hereby declare that:

Our residence, mailing address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled "Method and Device for Encrypting Multicast Service in Passive Optical Network System", the specification of which

- ☐ is attached hereto.
- ☒ was filed on 9/20/2011 as Application Serial Number 13/257,731 and was amended on _____ (if applicable)..
- ☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent or inventor's or plant breeder's rights certificate(s) or 365(a) of any PCT international application which designated at least country other than the United States of America, listed below and have also identified below any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing	Date of Issue	Priority Claimed Under 35 U.S.C. §119
China	201010102646.2	2010-01-25	N/A	Yes
PCT	PCT/CN2010/078611	2010-11-10	N/A	Yes

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys or agents with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 95957

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature Zhang Dezhi Date 2011.11.10.
 Full Name of First Inventor ZHANG Dezhi
 Family Name First Given Name Second Given Name

Residence Guangdong Province, P.R.China Citizenship China

Mailing Address : ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen City, Guangdong
Province 518057, P. R. China

Signature YUAN Liguang Date 2011.11.10
 Full Name of Second Inventor YUAN Liguang
 Family Name First Given Name Second Given Name

Residence Guangdong Province, P.R.China Citizenship China

Mailing Address : ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen City, Guangdong
Province 518057, P. R. China

ABSTRACT

A method for encrypting multicast services in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generating a public key, and using the public key to encrypt the multicast service data in a bearer channel and then transmitting the encrypted data, the multicast service data in the same one bearer channel being encrypted using the same public key; and said OLT sending the public key, which is used to encrypt the multicast service data, via a management control channel to an Optical Network Unit (ONU) which is activated successfully and requests to receive said multicast service data. A device for encrypting multicast services in a passive optical network system is also provided in the present invention. By applying the bearer channel encryption mechanism, the present invention is able to reduce the complexity of the OLT encryption mechanism and the ONU decryption mechanism on the premise of ensuring the encryption of the multicast services.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/24 (2006.01)

H04L 9/00 (2006.01)

H04N 7/173 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510103487.7

[43] 公开日 2006 年 11 月 22 日

[11] 公开号 CN 1866857A

[22] 申请日 2005.9.19

[21] 申请号 200510103487.7

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 赵 明 江 涛 谭培龙

[74] 专利代理机构 北京凯特来知识产权代理有限公司

司

代理人 郑立明

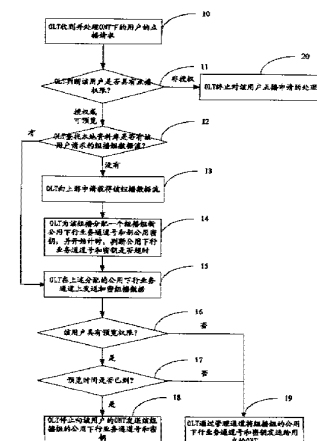
权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称

一种 PON 系统组播权限管控方法

[57] 摘要

本发明涉及通信技术领域一种 PON 系统组播权限管控方法，该方法通过在 OLT 上设置用户点播权限，对于已授权用户，OLT 为用户的 ONT 分配公用下行业务通道号和公用密钥，并定时更新公用下行业务通道号和公用密钥，且为具有预览权限的用户设置每次预览时间及规定时间内的预览次数，用来实现对组播业务权限的管控。本发明实现了 PON 网络接入系统用户点播过程的受控，使只有拥有相应权限的用户才能得到相应的服务，使得在 PON 系统中能够开展商业的视频点播业务。



1、一种PON系统组播权限管控方法，其特征在于，包括：

A、无源光网络PON系统在光网络线路终端OLT设置用户点播权限；

B、在用户开展组播业务过程中，OLT为具有点播权限的用户分配用于开展组播业务的组播组公用下行业务通道号及公用密钥，并定时的更新。

2、如权利要求1所述的PON系统组播权限管控方法，其特征在于，所述的用户点播权限可以根据用户的光网络用户终端ONT的PONID确定。

3、如权利要求1或2所述的PON系统组播权限管控方法，其特征在于，所述的用户权限包括：授权、非授权和/或可预览。

4、如权利要求3所述的PON系统组播权限管控方法，其特征在于，所述步骤A还包括：

A1、为可预览的用户设置每次预览时间和/或限制规定时间内的预览次数。

5、如权利要求4所述的PON系统组播权限管控方法，其特征在于，所述步骤B包括：

B1、确定所述用户具有预览权限，且预览时间和/或规定时间内预览次数没到规定上限；

B2、OLT发送所述公用下行业务通道号及公用密钥。

6、如权利要求5所述的PON系统组播权限管控方法，其特征在于，所述步骤B1包括：

B11、根据设置的用户点播权限确定所述用户为授权用户。

7、如权利要求1所述的PON系统组播权限管控方法，其特征在于，所述步骤B包括：从分配公用下行业务通道号及公用密钥开始计时，每达到规定时间更新所述公用下行业务通道号。

8、如权利要求1所述的PON系统组播权限管控方法，其特征在于，所述步骤B包括：从分配公用下行业务通道号及公用密钥开始计时，每达到规定时间更新所述公用密钥。

9、如权利要求1所述的PON系统组播权限管控方法，其特征在于，还包括：

确定该用户为非授权用户，则OLT终止对该用户的点播申请的处理。

一种PON系统组播权限管控方法

技术领域

本发明涉及通信技术领域，尤其涉及一种PON系统组播权限管控方法。

背景技术

近年来，随着互联网的快速发展和个人电脑的普及，Internet数据流的激增加剧了接入部分的容量限制，接入网中传统的铜缆接入方式显然已经无法满足通信业务增长的需求。为此，光纤传输逐渐被广泛应用，光纤具有传输频带宽、容量大、损耗低、抗干扰能力强等优点，非常适合作为高速、宽带业务的传输媒体。在各种光接入技术中，PON（无源光网络）由于采用无源节点，具有敷设和运行维护成本低、对业务透明及易于升级等优点而备受关注。

PON作为一种新兴的宽带接入光纤技术，其在光分支点不需要节点设备，只需安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。

同时，随着通信技术的快速发展，数字多媒体信号也越来越受到人们的青睐，通过接入网络实现视频或音频的点播、组播和广播等应用，将更多地出现在目前和以后的网络接入系统中。

如图1所示为PON组播网络结构示意图，无源光网络从OLT（光网络线路终端）接入信号，通过ODN（光分配网络）分配给各用户端ONU/ONT，ONT为光网络用户终端，直接位于用户端；而ONU为光网络用户单元，与用

户端及其它的网络如以太网相连，在用户端可收看多媒体信号。其中OLT位于局端，ONU/ONT位于用户端，OLT到ONU/ONT的方向为下行方向，反之为上行方向。下行方向采用基于时分复用的组播方式，ODN将由OLT输入的光信号按功率平均分配到若干输出用户端，一般有1分16、1分32或1分64等分配方案。

该现有的组播视频点播操作过程参照图2所示，图2为一种通过PON接入系统进行组播视频点播的方法流程。图中，OLT为每个组播组分配一个独立公用下行业务通道，每个组播组只发送一份组播数据流，并且该组播数据流只有那些下挂的用户发出了点播申请的ONT才能正常在该通道上接收。OLT还要为每个组播组产生一个公共密钥，在发送组播数据流时，利用该密钥进行加密；并将该密钥和公用业务通道号利用管理通道发送给具有组播接收权限的ONT，ONT利用该密钥在公用业务通道上对该组播数据流进行解密，接收并向用户转发该组播数据流。

不难看出，该方法只是实现了同一个PON口下的多个ONT下的用户发出点播申请后，OLT根据需要在每个PON口上只发送一份组播数据就可以实现多用户同时进行点播的方案。而没有考虑对用户的点播权限进行管理，ONT下的用户点播的过程完全不受控，因此，无法开展各种必须受控的组播业务，如视频点播业务，它要求在OLT上对每个ONT下的用户的每个组播组的点播权限分别进行控制，而在ONT下的用户不受控的情况下无法开展该视频点播业务。

因此，需要提供一种方法可以对点播端各用户的权限进行管控。

发明内容

鉴于上述现有技术所存在的问题，本发明的目的在于提供一种PON系统组播权限管控方法，通过在OLT上设置用户点播权限，对于已授权用户，

OLT为用户分配公用下行业务通道号和公用密钥，并定时更新公用下行业务通道号和公用密钥，且为具有预览权限的用户设置每次预览时间及规定时间内的预览次数，用来实现对组播业务权限的管控。

本发明的目的是通过以下技术方案实现的：

本发明提供一种PON系统组播权限管控方法，包括：

A、无源光网络PON系统在光网络线路终端OLT设置用户点播权限；

B、在用户开展组播业务过程中，OLT为具有点播权限的用户分配用于开展组播业务的组播组公用下行业务通道号及公用密钥，并定时的更新。

所述的用户点播权限可以根据用户的光网络用户终端ONT的PONID确定。

所述的用户权限包括：授权、非授权和/或可预览。

所述步骤A还包括：

A1、为可预览的用户设置每次预览时间和/或限制规定时间内的预览次数。

所述步骤B包括：

B1、确定所述用户具有预览权限，且预览时间和/或规定时间预览次数没到规定上限；

B2、OLT发送所述公用下行业务通道号及公用密钥。

所述步骤B1包括：

B11、根据设置的用户点播权限确定所述用户为授权用户。

所述步骤B包括：从分配公用下行业务通道号及公用密钥开始计时，每达到规定时间更新所述公用下行业务通道号。

所述步骤B包括：从分配公用下行业务通道号及公用密钥开始计时，每达到规定时间更新所述公用密钥。

还包括：

确定该用户为非授权用户，则OLT终止对该用户的点播申请的处理。

由上述本发明提供的技术方案可以看出，本发明实现了对PON网络接入系统用户点播权限的管控，将用户点播权限分为授权、非授权、可预览，使只有拥有相应权限的用户才能得到相应的服务，并使具有预览权限的用户短时间预览节目流，使得在PON系统中能够开展商业的视频点播业务。

附图说明

图1为现有技术PON组播网络结构示意图；

图2为现有技术PON接入系统进行组播视频点播的操作流程图；

图3为本发明PON接入系统实现用户点播权限管控操作流程图。

具体实施方式

本发明的核心思想是提供一种PON系统组播权限管控方法，通过在OLT上设置用户点播权限，对于授权用户，OLT为用户分配公用下行业务通道号和公用密钥，并定时更新，且为具有预览权限的用户设置每次预览时间及规定时间内的预览次数，用来实现对组播业务权限的管控。

本发明提供了一种PON系统组播权限管控方法，参照图3所示为本发明所述方法的操作流程图，该PON系统组播权限管控方法具体包括：

步骤10：OLT收到并处理ONT下的用户的点播请求；

用户可通过IGMP（互联网组管理协议）协议发送该点播请求；

步骤11：OLT对该用户进行鉴权；

可预先在OLT设置各用户点播权限，如配置各用户针对各个组播组的用户权限表，根据各用户的ONT的PONID规定各用户的点播权限，该用户权限表规定用户的点播权限分为：授权、非授权、可预览等三个级别，并对可预览的用户设置每次预览时间和/或限制规定时间内的预览次数；

OLT在收到用户的点播请求后，获取该用户的ONT的PONID，根据该PONID对照上述用户权限表确定该用户的点播权限；

步骤12：若上述用户已被授权或具有预览权限，则OLT查找本地资料库是否有该用户请求的组播组数据流；

OLT根据该用户的点播请求查找本地资料库中是否存在该用户请求的组播组数据流；所述本地资料库用于存储本地组播组数据流信息；

步骤13：若没有该组播组数据流，则OLT向上游设备申请获得该组播组数据流；

若OLT没有在本本地资料库中查找到该用户请求的组播组数据流，则OLT向上游设备申请获得该组播组数据流；所述上游设备包括路由服务器、宽带接入服务器等可以获得组播组数据流的网络设备；

步骤14：OLT为该组播组数据流分配一个新公用下行业务通道号和新公用密钥，并开始计时，判断公用下行业务通道号和密钥是否超时；

获取上述用户请求的组播组数据流后，OLT为该组播组数据流分配一个新公用下行业务通道号及新公用密钥，OLT在生成新的公用下行业务通道号及密钥后就开始计时，用于判断当前公用下行业务通道号和密钥是否超时，每达到规定时间更新该公用下行业务通道号及公用密钥，即OLT定时更换公用下行业务通道号及公用密钥，该规定时间值可根据需要确定；为实现起来简单，该更换操作可以只更换公用密钥，而保持公用下行业务通道号不变；

步骤15：OLT在上述分配的公用下行业务通道上发送加密组播数据流；

OLT完成上述操作后，在上述分配的公用下行业务通道上发送上述用户请求的组播组数据，并利用上述分配的新公用密钥对该组播组数据流进行加密；若上述步骤12中，OLT在本本地资料库中查找到该用户请求的组播组数据流，则直接进行步骤15的操作；

步骤16：上述操作完成后，判断该用户是否具有预览权限；

步骤17: 若所述用户具有预览权限, 则判断预览时间及预览次数是否已到;

若所述用户具有预览权限, 则根据用户权限表中规定的每次预览时间及规定时间的预览次数判断该用户的预览时间和/或预览次数是否已到;

步骤18: 若判断上述预览时间和/或预览次数已到, 则OLT停止向该用户的ONT发送该组播组数据流的公用下行业务通道号和密钥;

当判断上述预览时间和/或预览次数已到, OLT停止向该用户的ONT发送该组播组数据流的公用下行业务通道号和密钥, 该用户的预览操作将被禁止;

步骤19: 若该用户没有预览权限, 即该用户权限为授权, 或上述判断该用户的预览时间及预览次数没有达到规定上限, 则OLT通过管理通道将组播组的公用下行业务通道号和密钥发送给用户的ONT;

由于该用户请求的组播组数据流已通过OLT分配的新公用下行业务通道发送, 该用户的ONT只有得到该公用下行业务通道号及密钥才能接收该组播组数据流信息;

步骤20: 若上述步骤11中判断该用户为非授权用户, 则OLT终止对该用户的点播申请的处理。

综上所述, 本发明实现了PON网络接入系统用户点播过程的受控, 使只有拥有相应权限的用户才能得到相应的服务, 使得在PON系统中能够开展商业的视频点播业务。

以上所述, 仅为本发明较佳的具体实施方式, 但本发明的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本发明揭露的技术范围内, 可轻易想到的变化或替换, 都应涵盖在本发明的保护范围之内。因此, 本发明的保护范围应该以权利要求的保护范围为准。

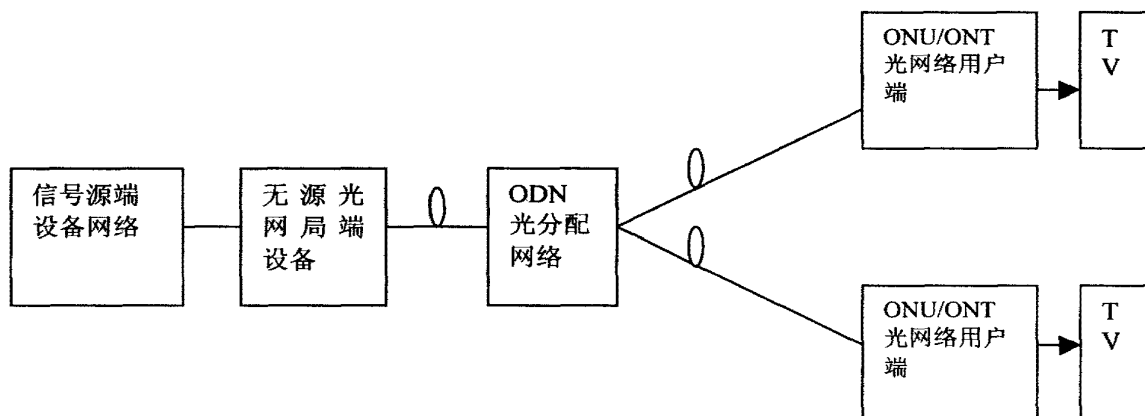


图1

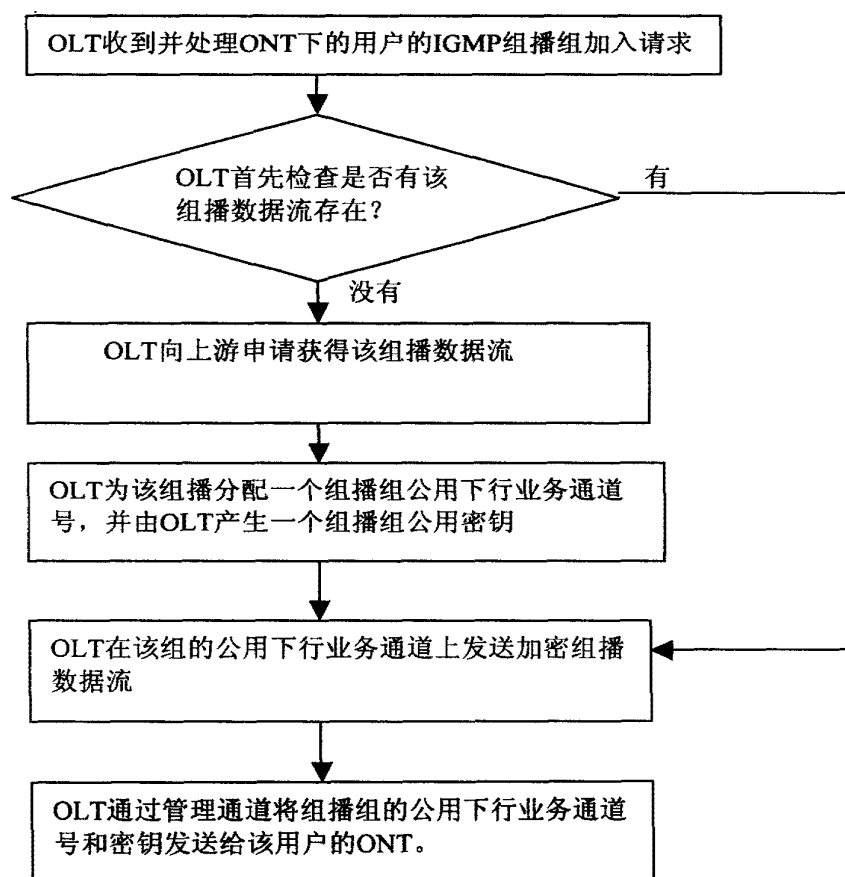


图2

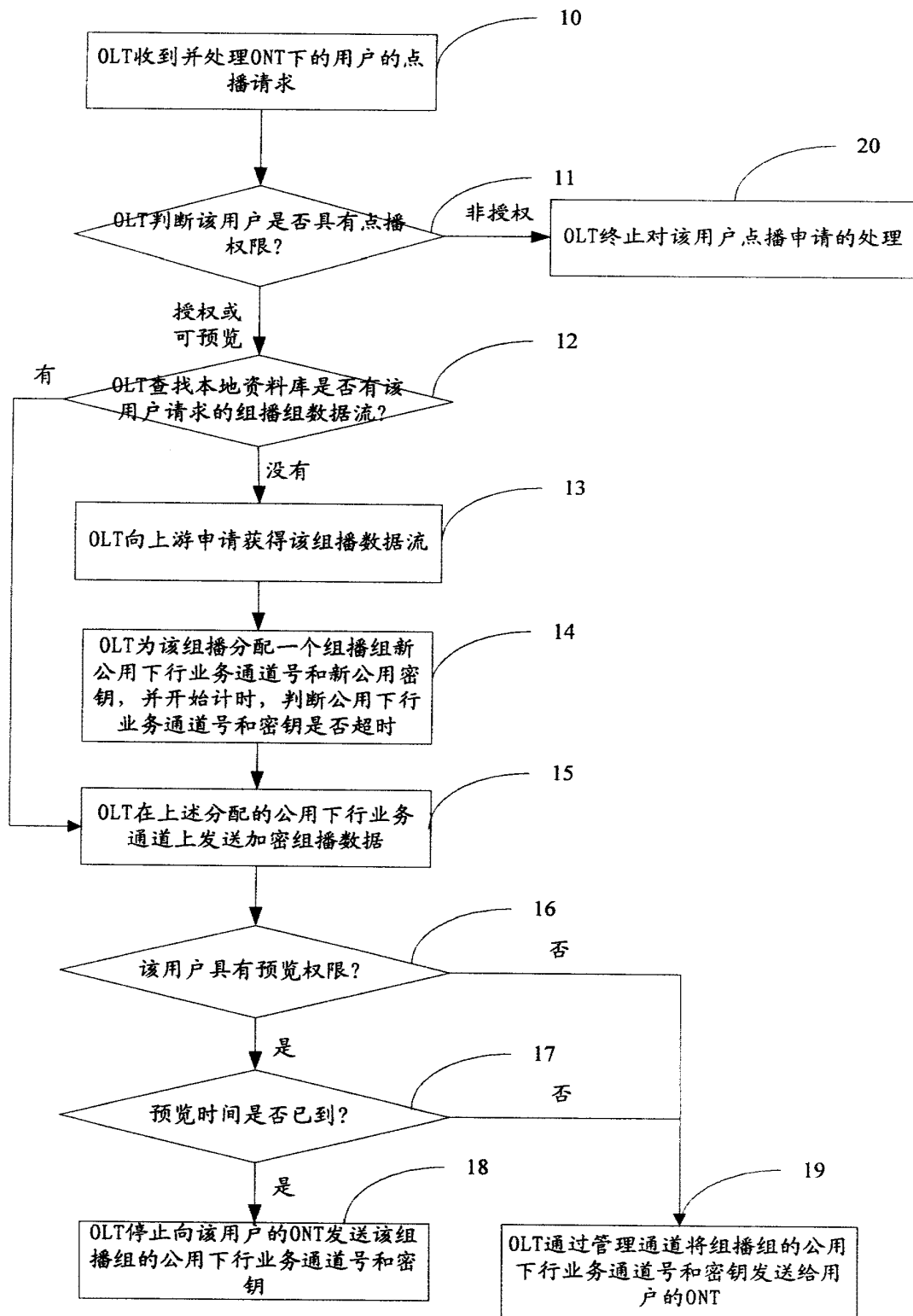


图3

Method and Device for Encrypting Multicast Service in Passive Optical Network System

Technical Field

The present invention relates to the field of optical communication, and more especially, to a method and device for encrypting multicast service data in passive optical network (PON) system.

Background of the Related Art

The structure of a PON is that one PON port corresponds to a plurality of optical network units (ONU) that are the PON terminal users, moreover, in the downlink, each ONU is able to receive all the data sent from the Optical Line Terminal (OLT) of office side, and “each ONU” mentioned here might be a legal user or a malicious user:

A user who has legal registration information, and can be activated by interacting messages with the OLT after physically connecting to a certain branch optical fiber of the PON is called a legal user;

A user who doesn't have legal registration information, and neglects the registration request sent from the OLT after physically connecting to a certain branch optical fiber of the PON, but only receives the downlink information is called a malicious user.

If it is a legal user, after connecting physically to one branch optical fiber and before being activated successfully, it still can receive various plaintext data packets sent from the OLT PON port. To date, the PON techniques define some encryption mechanisms, such as the Advanced Encryption Standard (AES) encryption mechanism in the Gigabit-Capable Passive Optical Network (GPON) system or the stirring encryption mechanism and the triple stirring encryption mechanism in the Ethernet Passive Optical Network (EPON) system and so on, these encryption mechanisms, however, are unicast encryption mechanisms. For multicast data (that is, only one service data is sent from the OLT PON port, and all users or part of users who meet the requirements receive and use the service data), there is no effective encryption mechanism right now. Generally, the operators set a universal key in the overall network range

to encrypt the services, whose disadvantage is that once the key is acquired by a malicious user, all service content in the overall network will be decrypted and stolen.

The method applied by the operators in the PON right now is to duplicate the multicast service data packets to each PON port and the unicast channel of the ONU, and the unicast mechanism is applied to carry out encryption so as to protect the multicast service data from being stolen by malicious users. This method, however, needs to send the key to each ONU, which increases the burden of the OLT.

Summary of the Invention

The technical problem to be solved by the present invention is to provide a method and device for encrypting multicast service in a passive optical network (PON) system to increase the security and reduce the complexity of OLT encryption mechanism and the burden of the OLT.

In order to solve the above technical problem, the present invention provides a method for encrypting multicast service in a PON system, and the method comprises:

an optical line terminal (OLT) generating a public key, and using the public key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same public key to carry out encryption; and

said OLT sending the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

Said method also comprises:

after said ONU obtains the public key, using said public key to decrypt the multicast service data that the ONU applies to receive in the bearer channel.

Said method also comprises:

said OLT generating the public key and setting an aging time for the public key , and after

the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data.

The step of said OLT sending the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data and actively sending the public key applied in encrypting the multicast service data to said ONU; alternatively

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the public key applied in encrypting said multicast service data to the ONU.

The multicast service data in different bearer channels might use different public keys or the same public key.

In the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where the multicast service data is encrypted with the public key.

In order to solve the abovementioned technical problem, the present invention also provides a device for encrypting multicast service in a passive optical network (PON) system, and the device comprises a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a public key;

said encryption unit is configured to: encrypt multicast service data born in a same one bearer channel with a same public key;

said sending unit is configured to: send the encrypted multicast service data, and send the public key used in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the public key, and when the aging time arrives, notify said key generation unit to regenerate a public key.

said sending unit is configured to apply a following method to send the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the public key applied in encrypting the multicast service data to said ONU; alternatively, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast service data, and then sending the public key applied in encrypting the multicast service data to the ONU.

Said sending unit is also configured to: at the same time when sending the public key to the ONU which is activated successfully and applies to receive the multicast service data, send the ONU a bearer channel identification of the bearer channel where the multicast service data is encrypted with the public key.

With the bearer channel encryption mechanism, the present invention reduces the complexities of the OLT encryption mechanism and the ONU decryption mechanism on the premise of guaranteeing the encryption of the multicast service. Compared with the multicast service encryption mechanism in the prior art, it limits the range affected by disclosing the key from the whole network to a certain PON port, thus improve the security of the multicast service content.

In addition, since the multicast service data born in the PON is transmitted after encrypted, and the key is only sent to the users that are activated successfully, the malicious users cannot acquire the key, nor the legal users before registration, thus it prevents illegal behaviors of the malicious users such as stealing the multicast service content, meanwhile, it does not affect the legal users normally using the encrypted multicast service after being activated.

Brief Description of Drawings

The accompanying figures here are used to further illustrate the present invention and are

a part of the application, and the illustrative embodiments of the present invention are used to illustrate the present invention rather than limit the present invention improperly. In the accompanying figures:

FIG. 1 is a flow chart of a first embodiment of the present invention;

FIG. 2 is a flow chart of a second embodiment of the present invention;

FIG. 3 is a flow chart of a third embodiment of the present invention;

FIG. 4 is a flow chart of a fourth embodiment of the present invention.

Preferred Embodiments of the Present Invention

The inventive concept of the present invention is that: the OLT generates a public key and uses the public key to encrypt the multicast service data in the bearer channel and then sends the encrypted data, the data in the same one bearer channel is encrypted with the same public key; said OLT sends the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data via a management control channel (such as the optical network terminal (ONT) management control interface (OMCI) or the operation administration maintenance (OAM)).

After the ONU acquires the public key, it uses the key to decrypt the multicast service data that the ONU applies to receive in the bearer channel.

Preferably, the OLT regularly maintains the public key, and generates the public key and sets an aging time (with a timer) for the public key, and after the aging time arrives, regenerates a public key and use the new public key to encrypt the multicast service data in the bearer channel, and sends the newly generated public key to the ONU that is activated successfully and applies to receive the multicast service data. The aging time for a plurality of public keys can be the same or different. Alternatively, the OLT can update the public key at anytime if needed.

Said bearer channel is a logical channel of the PON, and it can be the general encapsulation model (GEM) channel born by the GPON port or the logical link identification

(LLID) channel of the EPON port, and it is maintained and updated by the OLT.

Said management control channel might also be a logical channel of the PON, such as a physical layer operation administration maintenance (PLOAM) channel or an OMCI channel in the GPON system, or an extended OAM channel in the EPON system. Alternatively, a digital channel can be applied to send the public key.

The OLT can generate a plurality of public keys at the same time to encrypt the data in different bearer channels respectively. Preferably, the public keys of the bearer channels at the same one PON port might be the same or different, for example, a different public key can be set in each bearer channel, or the same public key can be used in part of the bearer channels.

When the OLT encrypts the multicast data in a plurality of bearer channels, and these bearer channels might send data to the same ONU, the OLT can send the ONU the bearer channel identification of the bearer channel where the multicast service data is encrypted with the public key at the same time when sending the ONU the public key, that is, sending the bearer channel identification of the bearer channel that bears the multicast service data to the ONU so that the ONU can decrypt the data. This does not exclude the case that the ONU finds out the bearer channel that uses this public key by carrying out decryption one by one.

The embodiments of the present invention will be illustrated in detail in combination with the accompanying figures. It should be noted that, without confliction, the embodiments in this application and the characteristics of the embodiments could be randomly combined.

The first embodiment

The present embodiment is an embodiment of transmitting the public key in the GPON system, and the application range is the overall GPON physical port, and as shown in FIG. 1, the procedure comprises:

Step 110. The OLT generates a public key to be used in the multicast service;

Step 120. The OLT encrypts the multicast data to be sent at the PON port and transmits the encrypted data;

Step 130. The ONU powers on, accesses the GPON, and initiates a registration to the OLT and applies for the multicast service;

the specific procedure of registration and multicast service application has been defined relevantly in the GPON protocol and will be omitted here.

Step 140. The OLT detects that the ONU is activated successfully and applies for multicast service, and sends the generated public key to the ONU;

there is a record in the OLT no matter whether the ONU is activated successful or not as well as no matter which kind of multicast service the ONU applies for.

According to its own policy, the OLT sends the public key to the ONU after it detects that the ONU successfully applies for the multicast service or as long as it detects that the ONU applies for the multicast service.

The OLT can use the PLOAM channel in the GPON protocol, the OMCI channel or other channel (such as a digital channel) to send the multicast public key to the ONU that is activated successfully.

Step 150. After the ONU receives the public key for multicast encryption, it carries out decryption on all downlink multicast services with this key.

The second embodiment

The present embodiment is an embodiment of transmitting the public key and updating the key in the EPON system, and the application range is the overall EPON physical port, and as shown in FIG. 2, the procedure comprises:

Step 210. The OLT generates a public key to be used in the multicast service, and sets a timer T1 for this public key;

the timer is used to control the aging time of the public key.

Step 220. The OLT encrypts the multicast data to be sent at the PON port and transmits the encrypted data;

Step 230. The ONU powers on, accesses the EPON, and initiates a registration to the OLT and applies for the multicast service;

the specific procedure of registration and multicast service application has been defined

relevantly in the EPON protocol and will be omitted here.

Step 240. The ONU requests the OLT to send a public key of multicast service;

Step 250. After the OLT receives the request of the ONU, if it searches out that the ONU is in the state of successful registration and applies for the multicast service, then the OLT sends the generated public key to the ONU;

according to its own policy, the OLT sends a public key to the ONU after it detects that the ONU successfully applies for the multicast service or as long as it detects that the ONU applies for the multicast service.

Step 260. After the ONU receives the public key for multicast encryption, it carries out decryption on all downlink multicast services with this key.

Step 270. When the time set in the timer T1 arrives, the OLT regenerates a new public key and resets the timer T1 (so as to update the key after the time set in the timer T1 arrives again).

When there is another ONU requesting the OLT to send the public key of the multicast service, the OLT sends the newly generated public key to the ONU that requests the public key. Moreover, the OLT also needs to update the public key for the ONU to which the public key has been sent.

The OLT can use the management control channel (such as the extended OAM channel) in the EPON system or a digital channel to transmit the generated multicast public key to the ONU that is activated successfully.

The third embodiment

The present embodiment is an embodiment of rejecting a malicious user trying to access the service in the GPON system, and the application range is the overall GPON physical port, and as shown in FIG. 3, the procedure comprises:

Step 310. The OLT generates a public key to be used in the multicast service;

Step 320. The OLT encrypts the multicast data to be sent at the PON port and transmits the encrypted data;

Step 330. A malicious user ONU accesses the GPON;

The malicious user might not initiate a registration after accessing the GPON, and once it does, the registration must be unsuccessful and the malicious user cannot apply for the multicast service.

Step 340: the malicious user ONU requests the OLT to send the public key of the multicast service;

Step 350: after the OLT receives the request, it searches out that the ONU is not activated successfully and rejects to send the public key of the multicast.

Right now, the malicious ONU cannot acquire the public key of the multicast, thus it cannot decrypt the multicast service content, and the operators prevent the malicious users from stealing the content.

The fourth embodiment

The present embodiment is an embodiment of transmitting the public key in the GPON system, and the application range is one GEM channel corresponding to a certain multicast service in the GPON physical port, and the ONU in this embodiment only applies for the multicast service in the first GEM channel, and as shown in FIG. 4, the procedure comprises:

Step 410. The OLT generates a multicast public key A to be used in the first GEM channel and generates a multicast public key B to be used in the second GEM channel;

Step 420. The OLT uses the public key A to encrypt the multicast service data born in the first GEM channel and transmits the encrypted data, and all the ONUs in this channel share the public key A;

Step 430. The OLT uses the public key B to encrypt the multicast service data born in the second GEM channel and transmits the encrypted data, and all the ONUs in this channel share the public key B;

The executing order of the abovementioned steps 420 and 430 is not fixed.

Step 440. The ONU powers on, accesses the GPON, and initiates a registration to the OLT and applies for the multicast service;

Step 450. The OLT detects that the ONU is activated successfully and applies to receive the multicast service in the first GEM channel, then the OLT sends the public key A and the corresponding first GEM channel identification to the ONU;

in other embodiments, the ONU might also actively initiate a key request.

According to its own policy, the OLT might send the public key to the ONU after it detects that the ONU successfully applies for the multicast service or as long as it detects that the ONU applies for the multicast service.

Step 460. After the ONU receives the public key A and the corresponding first GEM channel identification, it decrypts the multicast service data transmitted in the first GEM channel.

Since ONU1 does not receive the public key B, it cannot decrypt the downlink data in the second GEM channel. It can be seen that when the same one ONU receives a plurality of multicast services that are born in different bearer channels, the OLT needs to send the ONU the bearer channel identification corresponding to the public key at the same time when sending the public key.

The OLT can use the PLOAM maintenance channel in the GPON protocol, the OMCI management channel or other channel to send the multicast public key to the ONUs that are activated successfully.

One public key can be used in one GEM channel or a plurality of GEM channels, that is, several GEM channels share one key.

The OLT for implementing the abovementioned method comprises a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a public key;

said encryption unit is configured to: encrypt the multicast service data born in the same one bearer channel with the same public key;

said sending unit is configured to: send the encrypted multicast service data, and send the public key used in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data via the management control

channel.

Preferably, the device also comprises:

an aging time setting unit, which is configured to: set an aging time for the public key generated by the key generation unit, and when the aging time arrives, notifying the key generation unit to regenerate a public key.

Said sending unit is also configured to: at the same time when sending the public key to the ONU that is activated successfully and applies to receive the multicast service data, send the ONU the bearer channel identification of the bearer channel where the multicast service data is encrypted with the public key.

Said sending unit is also configured to: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively send the public key applied in encrypting the multicast service data to said ONU; alternatively, after receiving a key request from the ONU, judge that the ONU is activated successfully and applies to receive the multicast service data, and then send the ONU the public key applied in encrypting the multicast service data.

It is understood by those skilled in the field that some or all steps in the abovementioned method can be implemented by instructing the relevant hardware by program, and said program can be stored in the computer readable storage media, such as read only memory, a magnetic disk or an optical disk. Optionally, some or all steps in the abovementioned embodiment can be implemented with one or more integrated circuits. Correspondingly, each module/unit in the abovementioned embodiments can be implemented in the form of hardware or software function modules. The present invention is not limited to any combination of hardware and software in any special form.

The above description is the preferred embodiments of the present invention rather than restriction of the present invention, and for those skilled in the field, there are various modifications and variations in the present invention. Without departing from the spirit and essence of the present invention, all these types of modification, equivalent replacement or variations should belong to the protection scope of the present invention.

Industrial Applicability

With the bearer channel encryption mechanism, the present invention reduces the complexities of the OLT encryption mechanism and the ONU decryption mechanism on the premise of ensuring the encryption of the multicast service. Compared with the multicast service encryption mechanism in the prior art, it limits the range affected by disclosing the key from the whole network to a certain PON port, thus improve the security of the multicast service content.

In addition, since the multicast service data born by the PON is transmitted after encrypted, and the key is only sent to the users that are activated successfully, the malicious users cannot acquire the key, nor the legal users before the registration, thus it prevents illegal behaviors of the malicious users, such as stealing the multicast service content, and it does not affect the legal users normally using the encrypted multicast service after being activated successfully at the same time.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-228668
(P2000-228668A)

(43) 公開日 平成12年8月15日 (2000.8.15)

(51) Int. Cl. ⁷	識別記号	F I	7-31-1)* (参考)
H 0 4 L 12/28		H 0 4 L 11/20	D
12/18		H 0 4 Q 3/00	
H 0 4 Q 3/00		H 0 4 L 11/18	

審査請求 有 請求項の数28 ○L (全 12 頁)

(21) 出願番号 特願2000-15669(P2000-15669)
 (62) 分割の表示 特願平10-14519の分割
 (22) 出願日 平成10年1月27日 (1998.1.27)

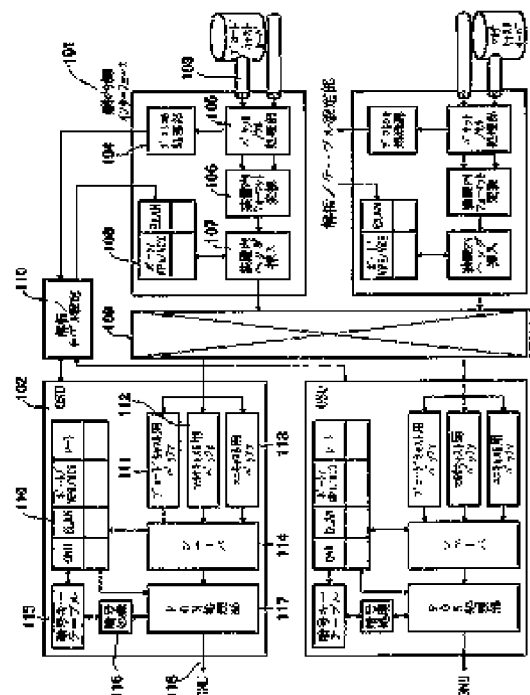
(71) 出願人 000004237
 日本電気株式会社
 東京都港区芝五丁目7番1号
 (72) 発明者 佐藤 むつみ
 東京都港区芝五丁目7番1号 日本電気株式会社内
 (74) 代理人 100082935
 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 パケット送信装置及び方法、パケット送出装置、パケット受信装置及び方法並びにパケット伝送システム

(57) 【要約】

【課題】 セキュリティ上問題を生じさせず、トラフィック増大、各ONUへの割り当て帯域の減少を招くことなくATM-PONによるユニキャスト、ブロードキャスト、マルチキャストを行う。

【解決手段】 OSU102は、各ONUのONU_ID、暗号キーと、各ELANの識別情報、暗号キーをテーブル110、暗号キーテーブル115に記憶する。ブロードキャスト時は、その旨をONU_IDとしてATMセルに付加してPONに送出し、マルチキャスト時には、その対象であるELANの識別情報をATMセルに付加後、当該ELANに対応した暗号キーで暗号処理を施し、マルチキャストである旨をONU_IDとして付加してPONに送出し、ユニキャスト時には、暗号処理後、当該ONUのONU_IDをATMセルに付加してPONに送出する。



【特許請求の範囲】

【請求項1】 ATM網に接続されたパッシブ光ネットワーク内の光ネットワーク装置に前記ATM網から光加入者装置を介してATMセルを伝送する方法であって、マルチキャストを行う際に、前記光加入者装置から前記パッシブ光ネットワークに、マルチキャストの対象である光ネットワーク装置のグループ毎に単一の通報を送出する工程を含むことを特徴とするATMセルの伝送方法。

【請求項2】 ATM網に接続されたパッシブ光ネットワーク内の光ネットワーク装置に前記ATM網から光加入者装置を介してATMセルを伝送する方法であって、前記ATM網と前記パッシブ光ネットワークとの間に介在する光加入者装置が、

a. ユニキャストの対象である光ネットワーク装置について、当該光ネットワーク装置を特定する光ネットワーク装置識別情報と当該光ネットワーク装置に対応した暗号キーを記憶するとともに、マルチキャストの対象である光ネットワーク装置の各グループ毎に、当該グループを特定するエミュレーテッドローカルエリアネットワーク識別情報および当該グループに対応した暗号キーを記憶し、

b. 前記パッシブ光ネットワークに接続された全ての光ネットワーク装置に対してATMセルのブロードキャストを行う場合には、ブロードキャストである旨の識別情報を光ネットワーク装置識別情報として当該ATMセルに付加し、ATMPONフレームとして前記パッシブ光ネットワークに送出し、

c. 前記パッシブ光ネットワークに接続された特定のグループに属する各光ネットワーク装置に対してATMセルのマルチキャストを行う場合には、当該グループを特定するエミュレーテッドローカルエリアネットワーク識別情報を当該ATMセルに付加した後、当該グループに対応した暗号キーにより暗号処理を施し、マルチキャストである旨の識別情報を光ネットワーク装置識別情報として付加し、ATMPONフレームとして前記パッシブ光ネットワークに送出し、

d. 前記パッシブ光ネットワークに接続された特定の光ネットワーク装置に対してATMセルのユニキャストを行う場合には、当該ATMセルに対し、当該光ネットワーク装置に対応した暗号キーにより暗号処理を施し、当該光ネットワーク装置を特定する光ネットワーク装置識別情報を当該ATMセルに付加し、ATMPONフレームとして前記パッシブ光ネットワークに送出し、

前記パッシブ光ネットワークに接続された各光ネットワーク装置は、

e. 当該光ネットワーク装置に対してユニキャストが行われるときに使用されるユニキャスト用の暗号キーを記憶するとともに、マルチキャストの対象となる光ネットワーク装置の各グループのうち当該光ネットワーク装置

が属する各グループについて、マルチキャストが行われるときに使用されるマルチキャスト用の暗号キーを記憶し、

f. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、当該光ネットワーク装置に対応した光ネットワーク装置識別情報を含む場合には、当該光ネットワーク装置に対応したユニキャスト用の暗号キーを使用して当該ATMPONフレームに含まれるATMセルのユニキャスト受信を行い、

g. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、ブロードキャストである旨の識別情報を光ネットワーク装置識別情報として含む場合には、当該ATMPONフレームに含まれるATMセルのブロードキャスト受信を行い、

h. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、マルチキャストである旨の識別情報を光ネットワーク装置識別情報として含む場合には、前記各グループ毎に定められた各暗号キーを使用して当該ATMPONフレームに含まれるATMセルのマルチキャスト受信を行うことを特徴とするパッシブ光ネットワークを介したATMセルの伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、パッシブ光ネットワークを介したATMセルの伝送方法、ATM通信装置、光加入者装置および光ネットワーク装置に関する。

【0002】

【従来の技術】周知の通り、ATM(Asynchronous Transfer Mode)網は、B-ISDN(広域サービス統合デジタル網)を支える根幹技術である。そして、このATM網と、ONU(Optical Network Unit; 光ネットワーク装置)との間を結ぶ光加入者系ネットワークの1つとして、PON(Passive Optical Network; パッシブ光ネットワーク)がある。

【0003】ここで、ATM網では、網内の各拠点間にVP(Virtual Path; 仮想パス)およびVC(Virtual Channel; 仮想チャネル)を設定し、これらのVPおよびVCを介することにより、ATMセルを出発ノードから目的ノードへ伝送するものであり、基本的に1対1通信、すなわち、ユニキャストを前提としている。これに対し、PONは、共通の光ファイバを介して各ONUにセルを伝送するものであるため、ブロードキャストに適したネットワークである。従って、これらの性格の異なったATM網とPONとを結ぶためには、そのインタフェースとしての役割を果たすATM通信装置が必要となる。

【0004】

【発明が解決しようとする課題】さて、ATM-PONを含むATM網に対する要求として、送信側装置から1つのONUへセルを伝送するユニキャスト、送信側装置

から全てのONUへセルを送送するブロードキャストおよび送信側装置から特定のグループに属する複数のONUへセルを送送するマルチキャストを実行する機能についての要求がある。

【0005】従来よりATM網においてブロードキャストを行うための技術やPONにおいてマルチキャストを行うための技術が各種提案されていたが、これらはいずれも上記要求を満たすには機能的に不十分であり、上記要求に応える最適な装置はなかった。

【0006】例えば、特開平8-186565号公報は、ATM網においてマルチキャストを行うための技術を開示している。この技術においては、パケット処理のレイヤで、マルチキャストの対象である全ての宛先アドレスを1つのパケット中に挿入してATM側に送出するものであり、この送出時に、管理されている宛先アドレスに対応するVCのディスクリプタに従い、送出すべきVCがなくなるまでパケットをセルに分解し、送出する作業を繰り返す。

【0007】しかしながら、この技術はブロードキャスト用のパケットのセルをコピーして伝送するものであるため、この技術をATM-PONを含むATM網に適用したとすると、ATMレイヤでセル数が増えるという問題がある。また、ATM網にPONが組み合わされ、かつ、そのPONの分岐数が多い場合に、各ONUに割り当てられる帯域が小さくなってしまいう問題が生じる。

【0008】また、特開平7-202905号公報は、ネットワークをツリー状に構成し、各ノードではユーザセル用とブロードキャスト用で別々にFIFOを持ち、各ノードを多段接続することにより、ブロードキャストセルについては当該ブロードキャストセルが入力された入力インタフェース点を除く全ての入力インタフェース点に送出する技術を開示している。

【0009】しかしながら、この技術はブロードキャストには適しているがマルチキャストを考慮していないため、この技術をATM-PONを含むATM網に適用したとすると、マルチキャストの対象であるONU以外の他のONUにもセルが送られてしまい、セキュリティ上問題がある。

【0010】また、文献「Access Flexibility with Passive Double Star System」では、ATM-PONのレイヤでのブロードキャストを行う際に、セルのヘッダ部の宛先ONUをブロードキャストを示すIDとし、暗号処理をしないで送信を行うようにしている。

【0011】この技術の場合、マルチキャスト、ブロードキャストがサポートできないか、あるいはユニキャスト通信の場合にパケットが他のONUにまで漏れてしまうことになり、セキュリティ上問題がある。何故ならば、この技術では、ATMレイヤとの連携を行わず、PONの設定をユニキャスト設定か、ブロードキャスト設

定に固定して処理するからである。

【0012】以上説明したように、従来の技術はいずれも上記要求を満たすには機能的に不十分であり、ATM-PONを含むATM網において、ユニキャスト、ブロードキャストおよびマルチキャストを適切に行うことを可能にする手段は従来提供されていなかった。

【0013】この発明は以上の事情に鑑みてなされたものであり、ATM-PONを含むATM網においてセキュリティ上問題を生じさせることなく、かつ、トラフィックの増大、各ONUへの割り当て帯域の減少といった不具合を招くことなくユニキャスト、ブロードキャストおよびマルチキャストを適切に行うことを可能にするATM-PONにおけるセルの伝送方法、ATM通信装置、光加入者装置および光ネットワーク装置を提供することを目的としている。

【0014】

【課題を解決するための手段】上記課題を解決するため、本発明では、ATM網に接続されたパッシブ光ネットワーク内の光ネットワーク装置にATM網側からATMセルを送送する場合に、前記ATM網と前記パッシブ光ネットワークとの間に介在する光加入者装置が、

a. ユニキャストの対象である光ネットワーク装置について、当該光ネットワーク装置を特定する光ネットワーク装置識別情報と当該光ネットワーク装置に対応した暗号キーを記憶するとともに、マルチキャストの対象である光ネットワーク装置の各グループ毎に、当該グループを特定するエミュレーテッドローカルエリアネットワーク識別情報および当該グループに対応した暗号キーを記憶し、

b. 前記パッシブ光ネットワークに接続された全ての光ネットワーク装置に対してATMセルのブロードキャストを行う場合には、ブロードキャストである旨の識別情報を光ネットワーク装置識別情報として当該ATMセルに付加し、ATMPONフレームとして前記パッシブ光ネットワークに送出し、

c. 前記パッシブ光ネットワークに接続された特定のグループに属する各光ネットワーク装置に対してATMセルのマルチキャストを行う場合には、当該グループを特定するエミュレーテッドローカルエリアネットワーク識別情報を当該ATMセルに付加した後、当該グループに対応した暗号キーにより暗号処理を施し、マルチキャストである旨の識別情報を光ネットワーク装置識別情報として付加し、ATMPONフレームとして前記パッシブ光ネットワークに送出し、

d. 前記パッシブ光ネットワークに接続された特定の光ネットワーク装置に対してATMセルのユニキャストを行う場合には、当該ATMセルに対し、当該光ネットワーク装置に対応した暗号キーにより暗号処理を施し、当該光ネットワーク装置を特定する光ネットワーク装置識別情報を当該ATMセルに付加し、ATMPONフレー

ムとして前記パッシブ光ネットワークに送出し、前記パッシブ光ネットワークに接続された各光ネットワーク装置は、

e. 当該光ネットワーク装置に対してユニキャストが行われるときに使用されるユニキャスト用の暗号キーを記憶するとともに、マルチキャストの対象となる光ネットワーク装置の各グループのうち当該光ネットワーク装置が属する各グループについて、マルチキャストが行われるときに使用されるマルチキャスト用の暗号キーを記憶し、

f. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、当該光ネットワーク装置に対応した光ネットワーク装置識別情報を含む場合には、当該光ネットワーク装置に対応したユニキャスト用の暗号キーを使用して当該ATMPONフレームに含まれるATMセルのユニキャスト受信を行い、

g. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、ブロードキャストである旨の識別情報を光ネットワーク装置識別情報として含む場合には、当該ATMPONフレームに含まれるATMセルのブロードキャスト受信を行い、

h. 前記パッシブ光ネットワークを介して到来したATMPONフレームが、マルチキャストである旨の識別情報を光ネットワーク装置識別情報として含む場合には、前記各グループ毎に定められた各暗号キーを使用して当該ATMPONフレームに含まれるATMセルのマルチキャスト受信を行う。

【0015】

【発明の実施の形態】以下、図面を参照し、本発明の実施の形態について説明する。図1はこの発明の一実施形態であるATM通信装置の構成を示すブロック図である。このATM通信装置は、複数の網内側インタフェース101と、複数のATMPONのOSU（Optical Subscriber Unit；光加入者装置）102と、これらの接続を行うATMスイッチ109とを有している。ここで、各OSU102には、図2に示すONU（Optical Network Unit；光通信網装置）がPONを介して接続され、これらのOSUおよびONUによりATM-PONが構成されている。

【0016】網内側インタフェース101は、プロトコル処理部104、パケット／セル処理部105、装置内フォーマット変換部106、装置内ヘッダ挿入部107およびテーブル108を有している。

【0017】ここで、テーブル108は、ATMスイッチ109のスイッチング制御に必要な情報を記憶する手段である。このテーブル108には、網内側インタフェース101を経由する各論理コネクション毎のATMスイッチ109のポート番号、VPIおよびVCIが設定される。また、本実施形態では、各論理コネクション毎にユニキャスト用であるか、マルチキャスト用である

か、あるいはブロードキャスト用であるかが予め装置内の約束事として決められ、各論理コネクションの用途を示す値がELAN情報としてテーブル108に設定される。例えば当該論理コネクションがユニキャスト用であるときは「1」、ブロードキャスト用であるときは「2」という具合にELAN情報が設定される訳である。また、本実施形態では、PONを介してOSU102に接続された各ONUによりELAN（Emulated LAN；エミュレーテッドローカルエリアネットワーク）を構成し、このELANを構成する各ONUを対象としてマルチキャストを行うことができる。このようなマルチキャストに使用する論理コネクションについては、例えば「3」がELAN情報として設定される。また、マルチキャストの対象となるELANが複数グループ存在する場合がある。このような場合、各ELANへのマルチキャストに使用する各論理コネクションについては、各ELANのグループ毎に取り決められた「3」以降の値のうち該当するものがELAN情報として設定される。

【0018】装置内フォーマット変換部106および装置内ヘッダ挿入部107は、通信路103およびパケット／セル処理部105を経たATM網側からのATMセルを装置内フォーマットに変換し、ATMスイッチ109に供給する手段である。

【0019】図3において、301はATM網側から送られてくるATMセルのフォーマットを示すものである。この図に示すように、ATMセルは、ATMヘッダ303およびATMペイロード304により構成されている。このATMセルは、装置内フォーマット変換部106を通過することにより、符号302により示す装置内フォーマットに変換される。そして、このフォーマット変換後のセルは、装置内ヘッダ挿入部107を通過する際に必要な情報が挿入される。さらに詳述すると、テーブル108内の各論理コネクションに対応した情報のうち当該セルに対応した情報が装置内ヘッダ挿入部107により読み出され、この情報のうちスイッチングのためのポート番号、VPIおよびVCIが当該セルのATMヘッダ303内に挿入され、ELAN情報がELAN-ID（エミュレーテッドローカルエリアネットワーク識別情報）として当該セルに挿入されるのである。そして、この装置内ヘッダ挿入部107の処理を経たセルがATMスイッチ109に供給されるのである。

【0020】プロトコル処理部104は、通信路103を介してATM網側から受信した信号の処理を、対向する装置との間で予め決められたプロトコルに従って行うとともに、上位レイヤの制御プロトコルやNMS（Network Management System；ネットワーク管理システム）からの設定情報、あるいはシグナリングプロトコルの内容を解析／テーブル設定部110に通知する手段である。

【0021】ATMスイッチ部109は、以上説明した

網内インタフェース101から送出されたセルを各々の宛先に対応したOSU102に送出する。さらに詳述すると、ATMスイッチ部109は、網内インタフェース101から装置内フォーマットのセルを受け取ると、そのELAN_IDに基づき、当該セルがブロードキャストの対象であるか、マルチキャストの対象であるか、ユニキャストの対象であるかを判定する。そして、ATMスイッチ部109は、ブロードキャストの対象であるセルについては必要なだけセルのコピーを作成し、全ての出力ポートから出力する。また、マルチキャストの対象であるセルについては、その宛先である具体的なELANを指定する値が当該セル内にELAN_IDとして含まれている。従って、そのようなELANに対応したものを含む適当な複数の出力ポートから当該セルを出力する。また、ユニキャストの対象であるセルについては、その宛先に対応したものを含む適当な複数の出力ポートから出力する。

【0022】OSU102は、テーブル110、ブロードキャスト用バッファ111、マルチキャスト用バッファ112、ユニキャスト用バッファ113、シェーパ114、暗号キーテーブル115、暗号処理部116およびPON処理部117を有している。

【0023】テーブル110には、網内側インタフェース101のテーブル108と同様なELAN情報、ポート番号、VPIおよびVCIの他、セル送出時のレート、宛先のONUを指定するONU_ID（光ネットワーク装置識別情報）が記憶される。

【0024】ATMスイッチ109から送られてくるセルは、そのELAN_IDに基づきブロードキャスト用であるか、マルチキャスト用であるか、ユニキャスト用であるかが判断され、ブロードキャスト用バッファ111、マルチキャスト用バッファ112またはユニキャスト用バッファ113のうち当該セルに対応したバッファに蓄積される。

【0025】シェーパ114は、テーブル110に従って、各バッファ111～113に蓄積されたセルを読み出し、PON処理部117に引き渡す。PON処理部117は、このシェーパ114からセルを受け取り、ONU_IDの付加等を行い、ATMPONフレームとして通信路118を介して各ONUに送る。図3において、308はATMPONフレームのフォーマットを示すものである。この図に示すように、ATMPONフレームは、ONU_ID309を有している。

【0026】PON処理部117におけるATMPONフレームの作成および送出の方法は、送出対象がブロードキャスト用であるか、マルチキャスト用であるか、ユニキャスト用であるかにより異なっている。すなわち、次の通りである。

【0027】a. 送出対象がブロードキャスト用セルである場合

この場合、当該セルがブロードキャスト用であることを示す情報をONU_IDとして付加し、ATMPONフレームとして通信路118に送出する。このATMPONフレームは、通信路118に接続された全てのONUに同報される。

【0028】b. 送出対象がマルチキャスト用セルである場合

この場合、2通りの送出方法をとることができる。

【0029】(1) 第1の送出方法

この第1の送出方法では、マルチキャスト用バッファ112内のセルを読み出すと、まず、当該セルの宛先であるONUを探索する。次に当該セルをコピーすることにより、宛先である各ONUに対応した個数のセルを生成し、各セルに各ONUに対応した各ONU_IDを付加する。そして、各セルをATMレイヤで各ONUにユニキャストする。

【0030】(2) 第2の送出方法

この第2の送出方法をとる場合、各ELAN毎に暗号キーを取り決め、暗号キーテーブル115に登録しておくとともに、各ELANを構成する各ONUに対し、該当する暗号キーを予め渡しておく。OSU102では、シェーパ114によりマルチキャスト用バッファ112内のセルを読み出すと、PON処理部117はテーブル110から当該セルの論理コネクションに対応した情報を読み出す。そして、PON処理部117は、この読み出し情報内のELAN情報により宛先であるELANを判定し、このELANに割り当てられたVPIおよびVCIを当該セルのヘッダ部に挿入する。そして、暗号処理部116が、暗号キーテーブル115に登録された当該ELANに対応した暗号キーを用いて、当該セルに暗号処理を施す。PON処理部117は、この暗号処理後のセルに対し、マルチキャストであることを示す情報をONU_IDとして付加し、ATMPONフレームとして通信路118に送出する。このATMPONフレームは、実際の光レイヤではブロードキャストされる。

【0031】なお、以上説明した第1および第2の送出方法は、ネットワークに要求されるセキュリティと、対向するONUが複数の暗号キーを処理する機能があるか否かにより、いずれかを選択する。

【0032】c. 送出対象がユニキャスト用セルである場合

暗号キーテーブル115には、各ONU毎にユニキャスト用の暗号キーが予め登録されており、各ONUには、該当する暗号キーが予め渡されている。OSU102では、シェーパ114がユニキャスト用バッファ113内のセルを読み出すと、暗号処理部116は、このセルに対し、暗号キーテーブル115に登録された当該ONUに対応した暗号キーを用いて暗号処理を施す。PON処理部117は、この暗号処理後のセルに対し、宛先であるONUのONU_IDを付加し、ATMPONフレー

ムとして通信路118に送出する。すなわち、ユニキャストの場合はATMレイヤでセルの送信を行うものである。

【0033】以上がブロードキャスト、マルチキャストおよびユニキャストの各場合におけるATMPONフレームの作成および送出の方法の詳細である。

【0034】さて、各セルが通信路118を介してブロードキャスト、マルチキャストあるいはユニキャストされる際、各セルはテーブル110に設定された送出レートで送出される。従って、テーブル110に各論理コネクションに対応した送信レートを設定する場合には、その総和が通信路118の容量制限内に収まるようにしなければならない。本実施形態では、以下のように送信レートの決定を行う。

【0035】まず、ブロードキャストについてはユニキャスト相当の帯域に対応した送信レートを設定する。例えば、1Mbpsのブロードキャストサービスを行う場合には、その対象であるONUが8台である場合でも、1Mbpsの送信レートを設定すればよい。

【0036】また、ユニキャストについては、各々必要

な帯域分に対応した送信レートを設定する。
【0037】また、マルチキャストの場合は、上記第1または第2の送出方法のいずれによりセルの送出を行うかにより、送出レートの設定方法は異なったものとなる。すなわち、上記第1の送出方法を採用場合には、マルチキャストの対象となる各ONUの台数に対応した容量相当の送出レートを設定し、上記第2の送出方法を採用場合には、ブロードキャストの場合と同様、ONU1台分の容量相当の送出レートを設定する。

【0038】次に解析/テーブル設定部110について説明する。上述した網内側インタフェース101のプロトコル処理部104は、上位レイヤの制御プロトコルやNMS（Network Management System；ネットワーク管理システム）からの設定情報、あるいはシグナリングプロトコルの内容をこの解析/テーブル設定部110に通知する。解析/テーブル設定部110は、この通知を受けた条件をこのATM通信装置およびATMPONが受け付けることができるか否かの判断を行う。受け付け可能であるとの判断がなされた場合、解析/テーブル設定部110は、その内部に保有するテーブルおよび網内側

インタフェース101のテーブル108の設定およびOSUのテーブル110の設定を行う。各テーブル108および110に設定される内容については既に説明した通りである。

【0039】なお、上記受け付けが可能であるか否かの判断は、CAC（Connection Admission Control；コネクション受付制御）等のこのATM通信装置に備わっている別の機能により行ってもよく、あるいは外付けのサーバ等で行ってもよい。

【0040】次に図2を参照し、各ONUの構成および

動作について説明する。図2に示すように、各ONUは、テーブル群202、PON処理部201、同期処理部213およびANDゲート214を有している。

【0041】まず、テーブル群202は、ユニキャスト用テーブル203と、ブロードキャスト用ONU_IDレジスタ204と、マルチキャスト用テーブル205とにより構成されている。

【0042】ここで、ユニキャスト用テーブル203は、ONU_IDレジスタ206と、暗号キーレジスタ207とにより構成されている。ONU_IDレジスタ206には、当該ONUのONU_IDが予め格納される。また、暗号キーレジスタ207には、当該ONUに割り当てられた上述のユニキャスト用の暗号キーが予め格納される。

【0043】ブロードキャスト用ONU_IDレジスタ204には、OSU側においてブロードキャスト用のセルに付加される上記「ブロードキャストであることを示す情報」が予め格納される。

【0044】また、マルチキャスト用テーブル205は、ONU_IDレジスタ208と、暗号キーレジスタ209-1～209-nからなる暗号キーテーブルとにより構成されている。ONU_IDレジスタ208には、OSU側において上記第2の送出方法によるマルチキャストが行われる際にマルチキャスト用のセルに付加される上記「マルチキャストであることを示す情報」が予め格納される。暗号キーレジスタ209-1～209-nには、OSU側において上記第2の送出方法によるマルチキャストが行われる際に使用される暗号キーが予め格納される。すなわち、既に説明したように上記第2の送出方法では、宛先である各ELAN毎に取り決められた暗号キーによりセルの暗号化が行われるが、このONUではいずれのELANに属する場合でもマルチキャスト受信を行い得るよう各ELANに対応したマルチキャスト用の暗号キーが暗号キーレジスタ209-1～209-nに予め格納されるのである。なお、OSU側が上記第1の送出方法によりマルチキャストを行う場合には、ONU_IDレジスタ208および暗号キーレジスタ209-1～209-nは使用されず、ユニキャスト用のONU_IDレジスタ206が使用される。

【0045】次に、PON処理部201は、光レイヤ処理部210、ONU_IDフィルタ211および暗号処理部212を有している。

【0046】上述したOSU側からのATMPONフレームは、光レイヤ処理部210の処理を経た後、ONU_IDフィルタ211を介して暗号処理部212に送られる。このATMPONフレームの通過の際、ONU_IDフィルタ211は、テーブル群202内にONU_IDレジスタ204、208および206内の各ONU_IDとフレーム内のONU_IDとを比較し、当該フレームがブロードキャストされたものであるか、マルチ

キャストされたものであるか、ユニキャストされたものであるかを判定する。

【0047】ここで、フレームがブロードキャストされたものである場合には、ONU_IDフィルタ211を通過したATMPONフレームは、何等処理が施されることなく暗号処理部212を通過し、同期処理部213に送られる。

【0048】フレームがユニキャストされたものである場合には、ユニキャスト用の暗号キーレジスタ207に格納された暗号キーが暗号処理部212に送られる。そして、この暗号キーを用いてONU_IDフィルタ211を通過したATMPONフレームの復元処理が行われ、処理後のフレームが同期処理部213に送られる。ここで、ATMPONフレームが当該ONUに対応した暗号キーで暗号されている場合には、暗号処理部212による復元処理が正常に行われ、同期処理部213により正常に受理される。一方、ATMPONフレームが当該ONUに対応した暗号キー以外の暗号キーで暗号されている場合には、暗号処理部212の復元処理は正常に行われず、同期処理部213では同期はずれを起こす。このため、当該ATMPONフレームは廃棄されることとなる。

【0049】フレームが上記第2の送出方法によりマルチキャストされたものである場合には、マルチキャスト用の暗号キーレジスタ209-1～209-nに格納された各暗号キーが暗号処理部212に順次送られる。そして、暗号処理部212では、ONU_IDフィルタ211を通過したATMPONフレームについて、これらの各暗号キーを用いた復元処理が順次行われ、復元後のフレームが同期処理部213に送られる。ここで、暗号処理部212に供給される暗号キーがATMPONフレームの暗号化に使用した暗号キーと一致していない場合には、復元後のフレームを同期処理部213に送ったとしても同期はずれを起こし、当該フレームは廃棄される。しかしながら、ATMPONフレームの暗号化に使

用した暗号キー、すなわち、当該ATMPONフレームの宛先であるELANに対応した暗号キーが暗号キーレジスタ209-1～209-n内のいずれかから暗号処理部212に送られると、その時点で、当該暗号キーによるATMPONフレームの復元処理が正常に行われることとなり、同期処理部213では同期はずれを起こすことなく復元後のフレームの受理が行われる。

【0050】フレームが上記第1の送出方法によりマルチキャストされたものである場合には、そのマルチキャストの対象である1つのONUのONU_IDが当該フレームに含まれている。この場合には、上述したユニキャストされたフレームの場合と同様な処理が行われる。

【0051】

【発明の効果】以上説明したように、この発明によれば、セキュリティおよび帯域の有効利用の両方を損わないよう、ATM-PONを介したブロードキャスト、マルチキャストおよびユニキャストを行うことができるという効果がある。

【図面の簡単な説明】

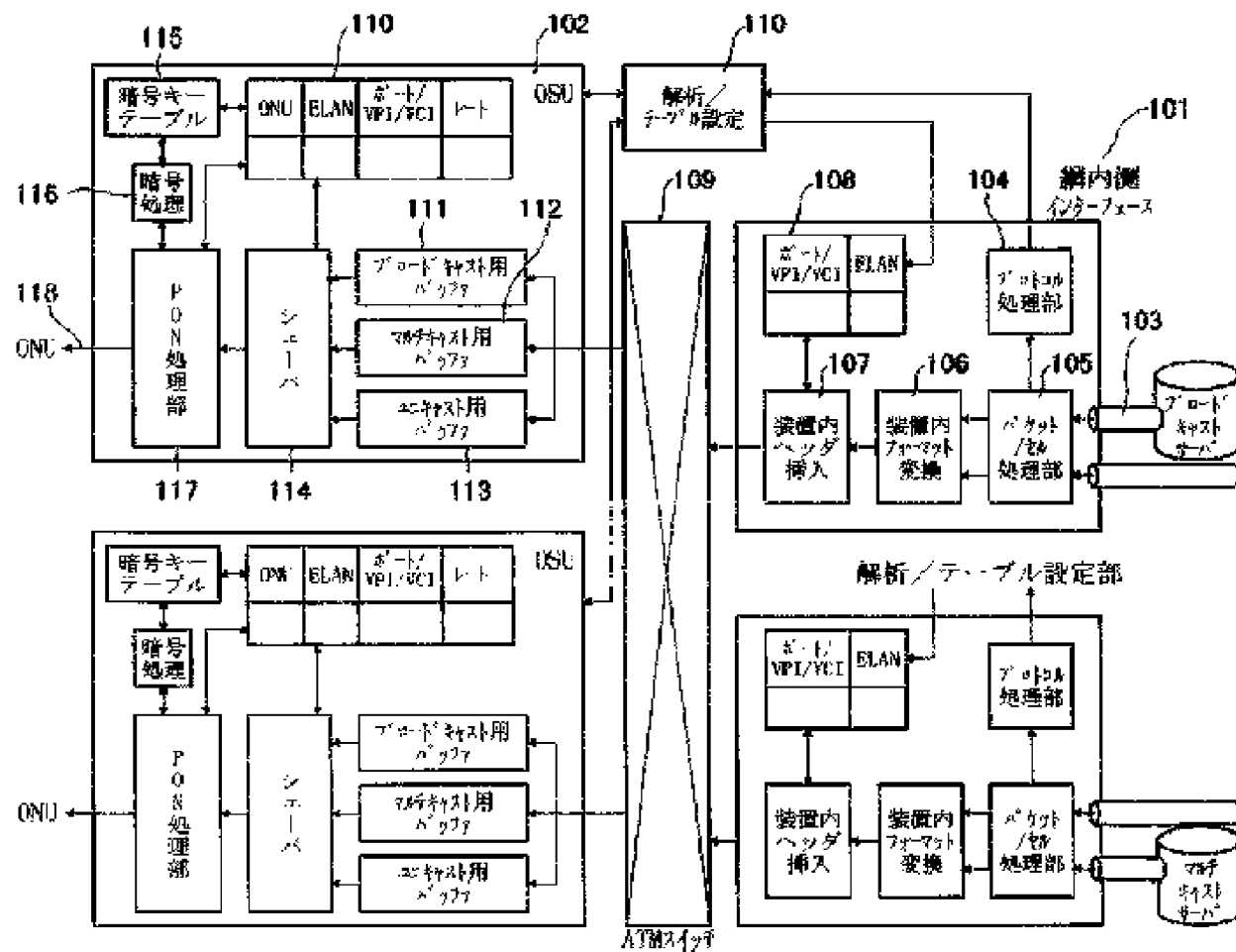
【図1】 この発明の一実施形態であるOSUを含むATM通信装置の構成を示すブロック図である。

【図2】 この発明の一実施形態であるONUの構成を示すブロック図である。

【図3】 上記ATM通信装置において取り扱うATMセル、装置内フォーマットのセル、ATMPONフレームの構成を示す図である。

【符号の説明】

102	OSU
110	テーブル
115	暗号キーテーブル
202	テーブル群
209-1～209-n	暗号キーレジスタ
207	暗号キーレジスタ
201	PON処理部

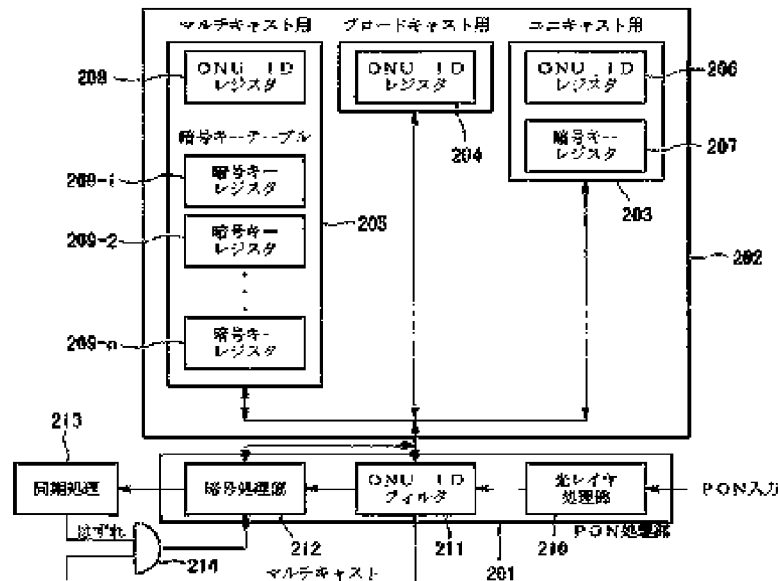


【図1】

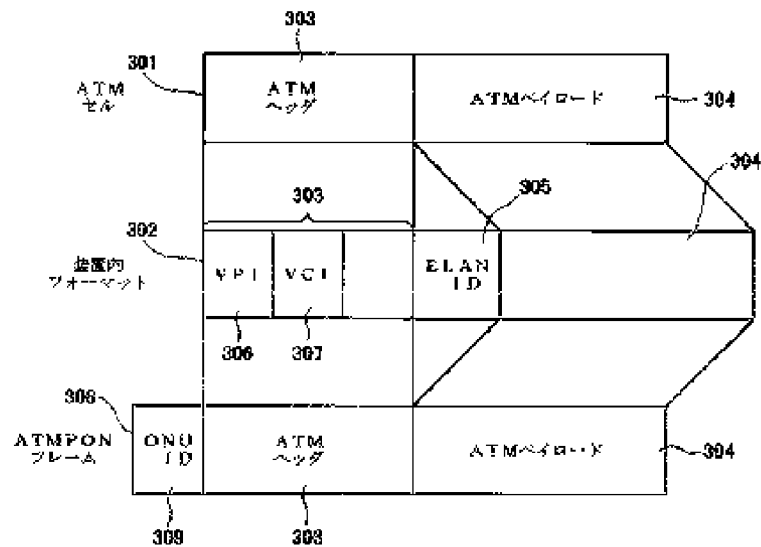
(8)

特開2000-228668

【図2】



【図3】



【手続補正書】

【提出日】平成12年4月24日（2000. 4. 24）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】 パケット送信装置及び方法、パケット送出装置、パケット受信装置及び方法並びにパケット伝送システム

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 入力される第1のバケット信号を第2のバケット信号に変換した後、前記第2のバケット信号を複数のバケット受信装置に同報するバケット送信装置であって、

前記バケット送信装置は、

前記複数のバケット受信装置の一部にマルチキャストする際には、前記第1のバケット信号に、マルチキャストすることを示す情報を付加して前記第2のバケット信号とするネットワーク処理部(117)を備えていることを特徴とするバケット送信装置。

【請求項2】 請求項1記載のバケット送信装置であって、

前記ネットワーク処理部は、マルチキャストする際には、前記情報の付加に先立ち、マルチキャスト先に対応した暗号キーを用いて前記第1のバケット信号を暗号化することを特徴とするバケット送信装置。

【請求項3】 請求項1又は請求項2のいずれかの請求項に記載されたバケット送信装置であって、

前記ネットワーク処理部は、前記複数のバケット通信装置全てに同報するブロードキャストの際には、前記第1のバケット信号に、ブロードキャストすることを示す情報を付加して前記第2のバケット信号とし、前記複数のバケット通信装置の1つのみに送信するユニキャストの際には、前記第1のバケット信号に、宛先である前記バケット受信装置の識別符号(ID)を付加して前記第2のバケット信号とすることを特徴とするバケット送信装置。

【請求項4】 請求項3記載のバケット送信装置であって、

前記ネットワーク処理部は、ユニキャストする際には、前記識別符号の付加に先立ち、宛先である前記バケット受信装置に対応した暗号キーを用いて前記第1のバケット信号を暗号化することを特徴とするバケット送信装置。

【請求項5】 請求項1乃至請求項4のいずれかの請求項に記載されたバケット送信装置であって、

前記バケット送信装置は、さらに、

前記第1のバケット信号がブロードキャスト用である場合に、前記第1のバケット信号を格納する第1のバッファ(111)と、

前記第1のバケット信号がマルチキャスト用である場合に、前記第1のバケット信号を格納する第2のバッファ(112)と、

前記第1のバケット信号がユニキャスト用である場合に、前記第1のバケット信号を格納する第3のバッファ(113)と、

前記第1乃至第3のバッファから前記第1のバケット信号を読み出して、前記ネットワーク処理部に供給するシ

ューバ(114)とを備えていることを特徴とするバケット送信装置。

【請求項6】 請求項1乃至請求項5のいずれかの請求項に記載されたバケット送信装置であって、前記第2のバケット信号がATMセルベースのフレームであることを特徴とするバケット送信装置。

【請求項7】 請求項6記載のバケット送信装置であって、前記バケット送信装置は、さらに、送出先のネットワークの伝送可能容量を上回らないように、前記第2のバケット信号の単位時間当たりの送出数を制御するテーブル(110)を備えていることを特徴とするバケット送信装置。

【請求項8】 入力される少なくとも1つの第1のバケット信号を第2のバケット信号に変換した後、前記第2のバケット信号を複数のバケット受信装置に同報するバケット送出装置であって、

前記バケット送出装置は、

複数の、請求項1乃至請求項7のいずれかの請求項に記載されたバケット送信装置(102)と、

前記少なくとも1つの第1のバケット信号を、前記複数のバケット送信装置のうち少なくとも1つに供給するバケットスイッチ(109)とを備えていることを特徴とするバケット送出装置。

【請求項9】 請求項8記載のバケット送出装置であって、

前記バケット送出装置は、さらに、

前記第1のバケット信号を所定の装置内フォーマットに変換するとともに、マルチキャスト、ブロードキャスト、ユニキャストの別を示す情報を付加する、少なくとも1つの網内側インターフェースを備えていることを特徴とするバケット送出装置。

【請求項10】 請求項8又は請求項9のいずれかの請求項に記載されたバケット送出装置であって、前記第2のバケット信号がATMセルベースのフレームであることを特徴とするバケット送出装置。

【請求項11】 請求項10記載のバケット送出装置であって、前記バケット送出装置は、さらに、送出先のネットワークの伝送可能容量を上回らないように、前記第2のバケット信号の単位時間当たりの送出数を制御するテーブル(110)を備えていることを特徴とするバケット送出装置。

【請求項12】 請求項11記載のバケット送出装置であって、前記テーブルは、さらに、前記バケットスイッチからの出力信号量を調節することを特徴とするバケット送出装置。

【請求項13】 バケット送信装置から出力され、マルチキャスト、ブロードキャスト、ユニキャストの別を示す伝送形態識別情報が付加されたバケット信号を受信するバケット受信装置であって、

前記バケット受信装置は、

前記伝送形態識別情報を格納するテーブル群(202)と、

該テーブル群から供給される前記伝送形態識別情報と、前記バケット信号に格納された前記伝送形態識別情報を順次比較するネットワーク受信処理部(201)とを備えていることを特徴とするバケット受信装置。

【請求項14】 請求項13記載のバケット受信装置であって、

前記ネットワーク信号処理部は、暗号処理部を備え、前記テーブル群は、さらに、自バケット受信装置にユニキャストされた前記バケット信号を復号する第1の暗号キーを格納する暗号キーレジスタと、自バケット受信装置を含んでマルチキャストされた前記バケット信号を復号する少なくとも1つの第2の暗号キーを格納する暗号キーレジスタとを含み、

前記暗号処理部は、前記伝送形態識別情報の照合の結果、前記バケット信号がユニキャストされたと判定された場合には、前記第1の暗号キーで前記バケット信号を復号し、前記バケット信号がマルチキャストされたと判定された場合には、前記少なくとも1つの第2の暗号キーで順次復号することを特徴とするバケット受信装置。

【請求項15】 請求項14記載のバケット受信装置であって、

前記バケット受信装置は、さらに、前記暗号処理部で復号された前記バケット信号に対しフレーム同期の確立を試み、失敗に終わった場合に、前記バケット信号を廃棄する同期処理部を備えていることを特徴とするバケット受信装置。

【請求項16】 請求項13乃至請求項15のいずれかの請求項に記載されたバケット受信装置であって、前記バケット信号がATMセルベースのフレームであることを特徴とするバケット受信装置。

【請求項17】 請求項1乃至請求項7のいずれかの請求項に記載されたバケット送信装置と、

請求項13乃至請求項16のいずれかの請求項に記載された少なくとも1つのバケット受信装置と、

前記バケット送信装置の出力信号を、前記少なくとも1つのバケット受信装置の各々に同報する同報型ネットワークとを備えていることを特徴とするバケット伝送システム。

【請求項18】 請求項17記載のバケット伝送システムであって、

前記同報型ネットワークは、放送型媒体を備えていることを特徴とするバケット伝送システム。

【請求項19】 請求項17記載のバケット伝送システムであって、

前記同報型ネットワークは、パッシブ光ネットワークを備えていることを特徴とするバケット伝送システム。

【請求項20】 第1のバケット信号を第2のバケット信号に変換した後、前記第2のバケット信号を複数のバ

ケット受信装置に同報するバケット送信方法であって、前記バケット送信方法は、

前記第1のバケットを受け付けるバケット受付工程と、前記複数のバケット受信装置の一部にマルチキャストする際には、前記第1のバケット信号に、マルチキャストすることを示す情報を付加して前記第2のバケット信号とする情報付加工程と、

前記第2のバケット信号を送出するバケット送出工程とを含んでいることを特徴とするバケット送信方法。

【請求項21】 請求項20記載のバケット送信方法であって、

前記バケット送信方法は、さらに、マルチキャストする場合、前記情報付加工程に先立ち、マルチキャスト先に対応した暗号キーを用いて前記第1のバケット信号を暗号化する第1の暗号化工程を含んでいることを特徴とするバケット送信方法。

【請求項22】 請求項20又は請求項21のいずれかの請求項に記載されたバケット送信方法であって、

前記バケット送信方法は、さらに、前記バケット受付工程に引き続き、前記第1のバケット信号が、マルチキャスト、前記複数のバケット通信装置全てに同報するブロードキャスト、又は前記複数のバケット通信装置の1つのみに送信するユニキャストのいずれの形態で送出すべきかを識別する伝送形態識別工程を含み、

前記情報付加工程において、ブロードキャストの際には、前記第1のバケット信号に、ブロードキャストすることを示す情報を付加して前記第2のバケット信号とし、ユニキャストの際には、前記第1のバケット信号に、宛先である前記バケット受信装置の識別符号(ID)を付加して前記第2のバケット信号とすることを特徴とするバケット送信方法。

【請求項23】 請求項22記載のバケット送信方法であって、

前記バケット送信方法は、さらに、ユニキャストする際には、前記情報付加工程に先立ち、宛先である前記バケット受信装置に対応した暗号キーを用いて前記第1のバケット信号を暗号化する第2の暗号化工程を含んでいることを特徴とするバケット送信方法。

【請求項24】 請求項20乃至請求項23のいずれかの請求項に記載されたバケット送信方法であって、前記第2のバケット信号がATMセルベースのフレームであることを特徴とするバケット送信方法。

【請求項25】 請求項24記載のバケット送信方法であって、前記バケット送信方法は、さらに、前記バケット送出工程に先立ち、送出先のネットワークの伝送可能容量を上回らないように、前記第2のバケット信号の単位時間当たりの送出数を制御する流量制御工程を含んでいることを特徴とするバケット送信方法。

【請求項26】 マルチキャスト、ブロードキャスト、ユニキャストの別を示す伝送形態識別情報が付加されたパケット信号を受信するパケット受信方法であって、前記パケット受信方法は、
前記パケット信号に格納された前記伝送形態識別情報からマルチキャスト、ブロードキャスト、ユニキャストの別を識別する伝送形態識別工程と、
前記伝送形態識別工程で前記パケット信号がユニキャストされたと判定された場合には、第1の暗号キーで前記パケット信号を復号し、前記パケット信号がマルチキャストされたと判定された場合には、少なくとも1つの第2の暗号キーで順次復号する暗号処理工程とを含んでい

ることを特徴とするパケット受信方法。

【請求項27】 請求項26記載のパケット受信方法であって、

前記パケット受信方法は、さらに、

前記暗号処理工程で復号された前記パケット信号に対しフレーム同期の確立を試み、失敗に終わった場合に、前記パケット信号を廃棄する同期処理工程を含んでいることを特徴とするパケット受信方法。

【請求項28】 請求項26又は請求項27のいずれかの請求項に記載されたパケット受信方法であって、前記パケット信号がATMセルベースのフレームであることを特徴とするパケット受信方法。

Electronic Acknowledgement Receipt

EFS ID:	11777355
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi ZHANG
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	06-JAN-2012
Filing Date:	
Time Stamp:	14:40:06
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment		no			
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	Joint_Declaration_and_POA.pdf	690682	no	2
			cab5fa1b5051b570adffd132474646220dbd0fd1		
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2		PCT_CN2010_078611_trans_of_spec_and_claims.pdf	131893	yes	16
			6537138312148503bc549e10bc7d2b9f58d610b8		

Multipart Description/PDF files in .zip description

		Document Description	Start	End
		Abstract	1	1
		Specification	2	13
		Claims	14	16

Warnings:

Information:

3	Drawings-only black and white line drawings	PCT_CN2010_078611_trans_of_drawings.pdf	360359	no	4
			f583f0f65e11c2b393534f9e0f4111f64a52d2f1		

Warnings:

Information:

4	Preliminary Amendment	confidential_preliminary_amendment_for_US.pdf	139555	no	6
			5b331faf6ff78c0b1c157685c3e22d1295ae8f0		

Warnings:

Information:

5	Information Disclosure Statement (IDS) Form (SB08)	updated_IDS_111101435_US.pdf	612345	no	4
			b8d35f1a2c2866702a83055b653e80fe362773e3		

Warnings:

Information:

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

6	Foreign Reference	CN1855834A.pdf	585333	no	13
			51eb900a2f765e99f11291981791e5e80a656459		

Warnings:

Information:

7	Foreign Reference	CN1866857A.pdf	510443	no	11
			faa5840ba91e7c9bfd96fa897a4b36e5e5d074c4		

Warnings:

Information:					
8	Foreign Reference	JP2000228668A.pdf	427077	no	12
			fa632944a806a302d61aca43c7b18a5b51fcad51		
Warnings:					
Information:					
Total Files Size (in bytes):				3457687	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731	
	Filing Date		2011-09-20	
	First Named Inventor	Dezhi ZHANG et al.		
	Art Unit			
	Examiner Name	Unknown		
	Attorney Docket Number		AFD111101435-US	

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1866857	CN	A	2006-11-22	HUAWEI TECHNOLOGIES CO., LTD		☐
	2	1855834	CN	A	2006-11-01	HUAWEI TECHNOLOGIES CO., LTD		☐
	3	2000228668	JP	A	2000-08-15	NEC CORP		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731
	Filing Date		2011-09-20
	First Named Inventor	Dezhi ZHANG et al.	
	Art Unit		
	Examiner Name	Unknown	
	Attorney Docket Number	AFD111101435-US	

If you wish to add additional Foreign Patent Document citation information please click the Add button				Add
NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
	1	International Search Report for PCT/CN2010/078611 dated January 21, 2011	☐	
If you wish to add additional non-patent literature document citation information please click the Add button				Add
EXAMINER SIGNATURE				
Examiner Signature			Date Considered	
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.				
<small> ¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached. </small>				

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2011-09-20
First Named Inventor	Dezhi ZHANG et al.
Art Unit	
Examiner Name	Unknown
Attorney Docket Number	AFD111101435-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ling Wu/	Date (YYYY-MM-DD)	2012-01-05
Name/Print	Ling Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Replace the Claims with the following amended Claims.

What is claimed is:

1. (Original) A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a public key, and using the public key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same public key to carry out encryption; and

said OLT sending the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

2. (Original) The method of claim 1, further comprising:

after obtaining the public key, said ONU using said public key to decrypt the multicast service data, which the ONU applies to receive, in the bearer channel.

3. (Currently amended) The method of claim 1 ~~or 2~~, further comprising:

said OLT generating the public key and setting an aging time for the public key, and after the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data.

4. (Original) The method of claim 1, wherein:

the step of said OLT sending the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the public key applied in encrypting the multicast service data to said ONU; or

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the public key applied in encrypting said multicast service data to the ONU.

5. (Original) The method of claim 1, wherein:

the multicast service data in different bearer channels use different public keys or the same public key.

6. (Currently amended) The method of claim 1 ~~or 2~~, wherein:

in the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

7. (Original) A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a public key;

said encryption unit is configured to: encrypt multicast service data born in a same one bearer channel with a same public key;

said sending unit is configured to: send the encrypted multicast service data, and send the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

8. (Original) The device of claim 7, wherein,

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the public key, and when the aging time arrives, notifying said key generation unit to regenerate a public key.

9. (Original) The device of claim 7, wherein:

said sending unit is configured to apply following methods to send the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the public key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast

service data, and then sending the public key applied in encrypting the multicast service data to the ONU.

10. (Currently amended) The device of claim 7 ~~or 9~~, wherein,

said sending unit is also configured to: send the public key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

11. (New) The method of claim 2, further comprising:

said OLT generating the public key and setting an aging time for the public key, and after the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data.

12. (New) The method of claim 2, wherein:

in the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

13. (New) The device of claim 9, wherein,

said sending unit is also configured to: send the public key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key.

REMARKS

In the preliminary amendment, as set forth above, the application is amended as follows.

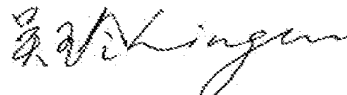
The abstract is shortened by deleting the last sentence.

The claims are amended as that: the multiple dependent claims 3, 6 and 10 are separated into several singularly dependent claims, and the generated claims are added in sequence following the last original claim 10.

Support for the preliminary amendment set forth above can be found in the claims and the specification including drawings as originally filed. Applicant asserts that no new matter is added.

It is believed that the application is in condition for allowance and such allowance is respectfully requested.

Respectfully submitted,

By:  _____

Ling Wu

Patent Agent for Applicant

Registration No. 66,304

Date: January 6, 2012

Ling Wu

1107 Bettstrail Way

Potomac, MD 20854

(301) 301-637-2202

(301) 251-0237 (fax)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

ZHANG, Dezhi et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **Unknown**

) Examiner: **Unknown**

PRELIMINARY AMENDMENTS

Mail Stop Amendment

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir or Madam:

Please amend the application as set forth herein.

Amendments to the Abstract begin on page 2 of this paper.

Amendments to the Claims begin on page 3 of this paper.

Remarks begin on page 6 of this paper.

Replace the Abstract with the following amended Abstract.

ABSTRACT

A method for encrypting multicast services in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generating a public key, and using the public key to encrypt the multicast service data in a bearer channel and then transmitting the encrypted data, the multicast service data in the same one bearer channel being encrypted using the same public key; and said OLT sending the public key, which is used to encrypt the multicast service data, via a management control channel to an Optical Network Unit (ONU) which is activated successfully and requests to receive said multicast service data. A device for encrypting multicast services in a passive optical network system is also provided in the present invention. ~~By applying the bearer channel encryption mechanism, the present invention is able to reduce the complexity of the OLT encryption mechanism and the ONU decryption mechanism on the premise of ensuring the encryption of the multicast services.~~

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/257,731		Filing Date 09/20/2011		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)		SMALL ENTITY ☐ OR			OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A		N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A		N/A		N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A		N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=	X \$	=	X \$	=	X \$	=
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=	X \$	=	X \$	=	X \$	=
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		TOTAL		TOTAL		TOTAL	
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)		SMALL ENTITY OR			OTHER THAN SMALL ENTITY		
AMENDMENT	01/06/2012	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0	X \$	=	X \$60=	0	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X \$	=	X \$250=	0	0
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE		TOTAL ADD'L FEE	0		
(Column 1)			(Column 2)		SMALL ENTITY OR			OTHER THAN SMALL ENTITY		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=	X \$	=	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=	X \$	=	=
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE		TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
/SHARAIN MORELAND/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/257,731			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA		RATE(\$)	FEE(\$)		RATE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A			N/A		
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A			N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A			N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	1	minus 20 =	*				x 60 =		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1	minus 3 =	*				x 250 =		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL			TOTAL 1120		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x
	Application Size Fee (37 CFR 1.16(s))							OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR	
				TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x
	Application Size Fee (37 CFR 1.16(s))							OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR	
				TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO. 13/257,731	FIRST NAMED APPLICANT Dezhi ZHANG	ATTY. DOCKET NO. AFD111101435-US
95957 Ling Wu 1107 Bettstrail Way Potomac, MD 20854		
INTERNATIONAL APPLICATION NO. PCT/CN2010/078611		
I.A. FILING DATE 11/10/2010		PRIORITY DATE 01/25/2010

CONFIRMATION NO. 6831
371 FORMALITIES LETTER



Date Mailed: 07/30/2012

**NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)**

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated Office (37 CFR 1.494):

- Priority Document
- Copy of the International Application filed on 09/20/2011
- English Translation of the IA filed on 09/20/2011
- Copy of the International Search Report filed on 09/20/2011
- Preliminary Amendments filed on 09/20/2011
- Information Disclosure Statements filed on 01/06/2012
- Oath or Declaration filed on 09/20/2011
- U.S. Basic National Fees filed on 09/20/2011
- Priority Documents filed on 09/20/2011

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Translation of the application into English. The current translation of the application into English is defective as described below. Note a processing fee will be required if submitted later than 30 months from the priority date.
 - Must submit a translation of original filed application.
- Processing fee of \$130 for providing the translation of the application and/or the Annexes later than 30 months from the priority date (37 CFR 1.492(i)).

SUMMARY OF FEES DUE:

Total additional fees required for this application is **\$130** for a Large Entity:

- **\$130** for English translation surcharge required.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

CHARITTA A SHELTON

Telephone: (571) 272-3926

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

ZHANG, Dezhi

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **Unknown**

) Examiner: **Unknown**

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

We received the Notification of Missing Requirements Under 35 U.S.C. 371 mailed on 7/30/2012. In the Notification, we were requested to submit the missing English Translation of application documents and pay the surcharge of \$130 for the submission later than 30 months from the priority date.

We reviewed our records and the Electronic Acknowledgement Receipt that we received from USPTO electronic filing system (EFS) on 01/06/2012 and we confirmed that we have submitted the English Translation of the application documents (Abstract, Specification, Claims and Drawings) on 01/06/2012. The submitted file for the Abstract, Specification and the Claims is PCT_CN2010_078611_trans_of_spec_and_claims.pdf.

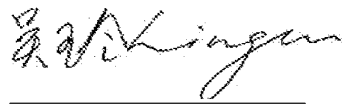
We further reviewed the image files that displayed on the PAIR, we found that our original

Filed: September 20, 2011

English Translation of the Abstract and the Claims was mistakenly replaced with the Abstract and Claims Amendment section from the Preliminary Amendment we submitted on the same date 01/06/2012. I made a call to EBC and reported to Agent 39 about this issue. He assured me that he EBC has received the English translation document, the QC center closed the file for rescan. The rescan must not have been done while the Notification of Missing Requirements was issued.

Since the issue was introduced by USPTO after the applicant submitted the required documents before 30 months from the priority date, we respectfully request USPTO re-review the submitted application documents, fix the image files issue, withdraw the request for the surcharge of \$130 and update the applicant with the new status.

Respectfully submitted,

By:  _____

Ling Wu

Patent Agent for Applicant

Registration No. 66,304

Date: Aug 17, 2012
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854
(301) 301-637-2202
(301) 251-0237 (fax)

Electronic Acknowledgement Receipt

EFS ID:	13523680
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi ZHANG
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	17-AUG-2012
Filing Date:	
Time Stamp:	14:24:29
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	Response_Missing_Docs.pdf	129133 6480ace0c807b9c4c0867eba510e19a14f4bb715	no	2

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.				
13/257,731	Dezhi Zhang	AFD111101435-US				
95957 Ling Wu 1107 Bettstrail Way Potomac, MD 20854		INTERNATIONAL APPLICATION NO. PCT/CN2010/078611				
		<table border="1"><tr><td>I.A. FILING DATE</td><td>PRIORITY DATE</td></tr><tr><td>11/10/2010</td><td>01/25/2010</td></tr></table>	I.A. FILING DATE	PRIORITY DATE	11/10/2010	01/25/2010
I.A. FILING DATE	PRIORITY DATE					
11/10/2010	01/25/2010					

CONFIRMATION NO. 6831
371 ACCEPTANCE LETTER



Date Mailed: 08/29/2012

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

<u>09/20/2011</u>	<u>07/25/2012</u>
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363). Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Copy of the International Application filed on 09/20/2011
- English Translation of the IA filed on 09/20/2011
- Copy of the International Search Report filed on 09/20/2011
- Preliminary Amendments filed on 09/20/2011
- Information Disclosure Statements filed on 01/06/2012
- Oath or Declaration filed on 09/20/2011
- U.S. Basic National Fees filed on 09/20/2011
- Priority Documents filed on 09/20/2011

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

CHARITTA A SHELTON

Telephone: (571) 272-3926



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.				
13/257,731	Dezhi Zhang	AFD111101435-US				
95957 Ling Wu 1107 Bettstrail Way Potomac, MD 20854		INTERNATIONAL APPLICATION NO. PCT/CN2010/078611				
		<table border="1"><tr><td>I.A. FILING DATE</td><td>PRIORITY DATE</td></tr><tr><td>11/10/2010</td><td>01/25/2010</td></tr></table>	I.A. FILING DATE	PRIORITY DATE	11/10/2010	01/25/2010
I.A. FILING DATE	PRIORITY DATE					
11/10/2010	01/25/2010					

**CONFIRMATION NO. 6831
371 WITHDRAWAL NOTICE**



Date Mailed: 08/29/2012

Letter Regarding a New Notice and/or the Status of the Application

If a new notice or Filing Receipt is enclosed, applicant may disregard the previous notice mailed on 07/30/2012. The time period for reply runs from the mail date of the new notice. Within the time period for reply, applicant is required to file a reply in compliance with the requirements set forth in the new notice to avoid abandonment of the application.

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If the reply is not filed electronically via EFS-Web, the reply must be accompanied by a copy of the new notice.

If the Office previously granted a petition to withdraw the holding of abandonment or a petition to revive under 37 CFR 1.137, the status of the application has been returned to pending status.

CHARITTA A SHELTON

Telephone: (571) 272-3926

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/257,731			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA		RATE(\$)	FEE(\$)		RATE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A			N/A		
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A			N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A			N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	13	minus 20 =	*				x 60 =		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 =	*				x 250 =		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL			TOTAL 1120		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x
	Application Size Fee (37 CFR 1.16(s))							OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR	
				TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x
	Application Size Fee (37 CFR 1.16(s))							OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR	
				TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									

<div> <div>MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET</div> <div>Substitute for Form PTO-1360 (For use with Form PTO/SB/06)</div> </div>							<div> <div>Application Number</div> <div>13257731</div> </div>		<div> <div>Filing Date</div> <div></div> </div>					
							<div> <div>Applicant(s)</div> <div>Dezhi ZHANG</div> </div>							
							* May be used for additional claims or amendments							
CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT			*		*		*		
	Indep	Depend	Indep	Depend	Indep	Depend		Indep	Depend	Indep	Depend	Indep	Depend	
1	1		1											
2		1		1										
3		2		1										
4		1		1										
5		1		1										
6		2		1										
7	1		1											
8		1		1										
9		1		1										
10		2		1										
11				1										
12				1										
13				1										
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														
35														
36														
37														
38														
39														
40														
41														
42														
43														
44														
45														
46														
47														
48														
49														
50														
Total Indep	2		2		0									
Total Depend	11	↙	11	↙	0	↙								
Total Claims	13		13		0									
51														
52														
53														
54														
55														
56														
57														
58														
59														
60														
61														
62														
63														
64														
65														
66														
67														
68														
69														
70														
71														
72														
73														
74														
75														
76														
77														
78														
79														
80														
81														
82														
83														
84														
85														
86														
87														
88														
89														
90														
91														
92														
93														
94														
95														
96														
97														
98														
99														
100														



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
13/257,731	09/20/2011		980	AFD111101435-US	13	2

CONFIRMATION NO. 6831

95957
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854

FILING RECEIPT



OC000000056184758

Date Mailed: 08/29/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Dezhi Zhang, Shenzhen City, CHINA;
Liquan Yuan, Shenzhen City, CHINA;

Assignment For Published Patent Application

ZTE CORPORATION, Shenzhen City, Guangdong Province, CN

Power of Attorney: The patent practitioners associated with Customer Number 95957

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/CN2010/078611 11/10/2010

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

CHINA 201010102646.2 01/25/2010

If Required, Foreign Filing License Granted: 08/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/257,731**

Projected Publication Date: 12/06/2012

Non-Publication Request: No

Early Publication Request: No

Title

Method and Device for Encrypting Multicast Service in Passive Optical Network System

Preliminary Class**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER**Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier

license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](https://www.selectusa.gov).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US

CONFIRMATION NO. 6831

PUBLICATION NOTICE



OC000000058007155

95957
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854

Title:Method and Device for Encrypting Multicast Service in Passive Optical Network System

Publication No.US-2012-0308006-A1

Publication Date:12/06/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	02/14/2013		
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			EXAMINER KORSAK, OLEG	
			ART UNIT 2492	PAPER NUMBER
			MAIL DATE 02/14/2013	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	13/257,731	ZHANG ET AL.	
	Examiner	Art Unit	
	OLEG KORSAK	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 September 2011.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-13 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-13 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☒ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) ☒ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____ | 4) ☐ Other: ____ |

DETAILED ACTION

This communication is responsive to the application # 13/257,731 filed on September 20, 2011. Claims 1-13 are pending and are directed toward a METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM.

Preliminary Amendment

Examiner acknowledges preliminary amendment filed on January 06, 2012. In the amendment claims 3, 6, 10 are amended and 11-13 are new.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. the form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. the abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "the disclosure concerns," "the disclosure defined by this invention," "the disclosure describes," etc.

The abstract of the disclosure is objected to because it has 164 words. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-13 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term “public key” in claims 1-13 is used by the claim to mean “common key”, while the accepted meaning is of the term “public key” in the art is one of the pair of public/private keys in asymmetric encryption. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. **Neither key can perform both functions by itself.** The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages. The term is indefinite because the specification does not clearly redefine the term.

For purposes of applying prior art the term “public key” was construed as “common key”.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 4-7, 9, 10, 12, 13 are rejected under 35 U.S.C. 102(b) as being *anticipated* by He (CN 1855834 November 1, 2006, translation by Dialog), hereinafter referred to as He.

As per **claim 1**, He teaches a method for encrypting multicast service in a passive optical network system (*a passive optical network pon technology, He, page 2*), the method comprising: an optical line terminal (OLT) generating a public key (*means of generating a key at the optical network line terminal, He, ABSTRACT*), and using the public key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same public key to carry out encryption (*said key is used as the public key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT*); and said OLT sending the public key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data (*while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream. He, ABSTRACT*).

As per **claim 2**, He teaches the method of claim 1, further comprising: after obtaining the public key, said ONU using said public key to decrypt the multicast service data, which the ONU

applies to receive, in the bearer channel (*And the key by using the other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal using the key to multicast data stream decoding receives the multicast data stream. He, Page 3*).

As per **claim 4**, He teaches the method of claim 1, wherein: the step of said OLT sending the public key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises: the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the public key applied in encrypting the multicast service data to said ONU; or the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the public key applied in encrypting said multicast service data to the ONU (*Can firstly the optical network user end of the optical network line terminal sends multicast application of optical network line road terminal to the multicast request processing according to user authority is determined whether to the optical network user end distributing multicast. If the user does not multicast authority optical network line terminal is not the multicast request. He, Page 3*).

As per **claim 5**, He teaches the method of claim 1, wherein: the multicast service data in different bearer channels use different public keys or the same public key (*By using this invention using the same service channels as same as the port id or vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6*).

As per **claim 6**, He teaches the method of claim 1, wherein: in the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key (*and the distribution of the multicast occupies a downlink service channel by channel number port id virtual channel identifier vpi or virtual channel identifier address to identify vci port is id. He, Page 5*).

As per **claim 12**, He teaches the method of claim 2, wherein: in the step of said OLT sending the public key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the public key (*the same service channels as same as the port id or vpi/vci of Service channel for the same multicast user transmitting multicast encrypted data streams. He, Page 6*).

Apparatus **claims 7, 9, 10, 13** are drawn to the apparatus corresponding to the method of using the same as claimed in claims 1, 2, 4-6, 12. Therefore apparatus claims 7, 9, 10, 13 correspond to method claims 1, 2, 4-6, 12, and are rejected for the same reasons of anticipation as used above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang (CN 1866857 November 22 2006, translation by Dialog), hereinafter referred to as He and Jiang respectively.

As per **claims 3 and 8**, He does not teach the aging time, Jiang, however, teaches the method of claim 1 further comprising: said OLT generating the public key and setting an aging time for the public key, and after the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data (*that receiver the user, OLT distributed of downlink service channel and a common key for user ONT, and timing updating the common downlink service channel and a common key, Jiang, ABSTRACT*).

He in view of Jiang are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang, p.4].

As per **claim 11**, He does not teach the aging time, Jiang, however, teaches the method of claim 2, further comprising: said OLT generating the public key and setting an aging time for the public key, and after the aging time arrives, it regenerating a new public key, and using the new public key to encrypt the multicast service data in the bearer channel, and sending the new public key to the ONU that is activated successfully and applies for the multicast service data (Steps: 14 OLT of the group multicast data stream assigns a new of downlink service channel number and new public key, and starting timing, wherein the output of downlink service channel

Art Unit: 2492

and a key, overtime. The gaining the group multicast data stream of the user request, OLT of the group multicast data stream assigns a new of downlink service channel number and new public key, a OLT generating the novel of downlink service channel number and a starting timing.

Jiang, Page 4)

He in view of Jiang are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang, p.4].

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US Patents

7,301,968

Teaches communication protocol for
PON topologies

US Pg. Pub

2008/0155255

Teaches encryption apparatus

2012/0128155

Teaches security in PON

2011/0029773

Teaches PON security

2010/0239252

Teaches control messages in EPON

2010/0174901

Teaches EPON networks

2004/0136372

Teaches protecting data in point to
multipoint network

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSACK whose telephone number is (571)270-1938. the examiner can normally be reached on Monday-Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. the fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/O. K./

Examiner, Art Unit 2492

/Saleh Najjar/

Supervisory Patent Examiner, Art Unit 2492



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6831

SERIAL NUMBER 13/257,731	FILING or 371(c) DATE 09/20/2011 RULE	CLASS 380	GROUP ART UNIT 2492	ATTORNEY DOCKET NO. AFD111101435-US		
APPLICANTS Dezhi Zhang, Shenzhen City, CHINA; Liquan Yuan, Shenzhen City, CHINA; ** CONTINUING DATA ***** This application is a 371 of PCT/CN2010/078611 11/10/2010 ** FOREIGN APPLICATIONS ***** CHINA 201010102646.2 01/25/2010 ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 08/24/2012						
Foreign Priority claimed ☒ Yes ☐ No 35 USC 119(a-d) conditions met ☒ Yes ☐ No Verified and Acknowledged <u>/OLEG KORSAK/</u> Examiner's Signature		☐ Met after Allowance OK Initials	STATE OR COUNTRY CHINA	SHEETS DRAWINGS 4	TOTAL CLAIMS 13	INDEPENDENT CLAIMS 2
ADDRESS Ling Wu 1107 Bettstrail Way Potomac, MD 20854 UNITED STATES						
TITLE Method and Device for Encrypting Multicast Service in Passive Optical Network System						
FILING FEE RECEIVED 980	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees		
				☐ 1.16 Fees (Filing)		
				☐ 1.17 Fees (Processing Ext. of time)		
				☐ 1.18 Fees (Issue)		
				☐ Other _____		
				☐ Credit		

Method for multicast via passive optical network**Patent Assignee (name, country):** HUAWEI TECH CO LTD, CN**Inventor (name, country):** JIANG TAO HE, CN**Patent Publications**

	Patent Number	Kind	Date	Application Number	Kind	Date		
Main Patent	CN 1855834	A	20061101	CN 200510034337	A	20050420		
H04L-0009/00	C	I	L	B	20060101	20061101	H	CN
H04L-0012/22	C	I	F	B	20060101	20061101	H	CN
H04L-0009/00	A	I	L	B	20060101	20061101	H	CN
H04L-0012/22	A	I	F	B	20060101	20061101	H	CN

Record Type (Availability): ABSTRACT; SPECIFICATION; CLAIMS ; IMAGE**Word Count:** 3241**Publication Language:** CHINESE**Translation Language:** Human Assisted Machine Translation to English**Abstract:**

The method comprises: in case of multi optical network users having multicast receiving right, the optical network line terminal allocates one downlink service channel for same multicast and sends one multicast bit-stream; the optical network line terminal opens the right to use said downlink service channel for said users having multicast receiving right in order to make said users capable of receiving said multicast bit-stream. The method also can be implemented by means of generating a key at the optical network line terminal, and said key is used as the public key of the multicast and is used to encrypt the multicast bit-stream while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream.

Legal Status Count: 3**Legal Status Information**

Date	Legal Event	Details
20091202	invention patent application deemed to be abandoned after publication	Effective Date: N/A

20061227	initiative for examination as to substance/operation of substantive examination	Effective Date: N/A
20061101	publication	Effective Date: N/A

Detailed Description:

A method for realizing passive optical network multicast method of

The technical field of

The invention claims a passive optical network pon technology field especially relates to a realize passive

Optical network multicast method of.

Background technology

In recent years with the internet of the fast development and personal computer and internet the normal data stream

The laser and increase the couple-on part of the content of limiting the access network the traditional method of copper cable the access way the natural

Has been not meet the communication service the requirement of increasing. Is composed of the optical fibre the transmission frequency bandwidth capacity is large

Loss is low the anti-jamming ability is strong and so on and it is very suitable to be used as high-speed broadband service transmission of media

Body. In all kinds of optical access technology in pon passive optical network because it adopts the passive node

Setting and operating and maintaining cost is low the service transparent and it is easy to upgrade and so on so as to prepare the attention.

Pon passive optical network is that the existing and future optical access with very prospect technology as

This utility model claims a new cover at last one kilometre of broadband access optical fibre technique the light branch points does not need to

Node only need to install a simple the optical splitter it can be used so it has advantages of saving optical fiber cable resource

Bandwidth resource share machine room it saves the investment of equipment high safety for establishing net and the speed is fast comprehensive building network

The cost is low and so on. At the same time the digital multimedia signal also becomes by the people * qing through

The access network achieves audio or video of broadcast multicast and broadcast the invention is suitable for the earth more is present at the

The front and back of the network access system.

As is shown in figure 1 is the pon multicast network structure conventional diagram of passive optical network from the optical network line

Road terminal olt end is connected with the input signal through the optical distribution network odn assigned to each user terminal and/or onu

Ont which is used as the light network user terminal directly the user terminal; And onu optical network is used for

User unit is connected with the user is also set the other network such as ethernet end of the user can watch multimedia

Signal. The local terminal olt is located on the onu/ont in which a user terminal olt the onu/ont

Is the direction the down direction is between the up direction. The down direction using based on time division multiplexing of

Broadcasting odn by olt it is composed of the input optical signal according to the power is evenly distributed in many for outputting

User terminal the common 1*16 1*32 or 1*64 and allocation scheme.

Such as picture 2 which is displayed in existing technology and the multicast copy master to sketch map multicast method is as follows

On olt end of processing multicast the multicast packet is copied into several multicast packet the multicast for

User terminal onu/ont are respectively connected with the corresponding multicast copying and.

The shortcomings of the current technology at each multicast channel has a plurality of user applies the olt the copied

Into a plurality of data packet the onu/ont transmission each onu/ont obtaining corresponding data

It so the occupy most of the downlink data width. Such as: Has 10 plurality of multicast channels flat

Has 10 user applies for setting data flow as 5mbit or s when descending bandwidth is occupied bandwidth as the:

$10 \times 10 \times 5 = 500$ mbit s and x.

The content of invention

The invention aims to solve the technique problem that: Overcomes the existing technology passive optical network multicast when

Used for a plurality of downlink data width is not enough the invention claims a method for realizing passive optical network multicast method for reducing

The group broadcast downlink transmission to the frequency band occupied band-width.

This invention is to solve said technical problem the adopted technical plan is as follows:

This utility model can realize passive optical network multicast the method of the multicast receiving authorization a plurality of light

Network user terminal optical network line terminal to the same multicast distributing a downlink service channel

Send only one multicast data stream; Optical network line the terminal has a broadcast receiving the authority optical network

User end opening of said downlink service channel the right of the optical network user terminal can receive the multicast

Data stream.

Can be composed of the optical network line terminal generates a key and the key as the multicast the Common key transmitting the multicast data stream when using the key to encrypt; And the key by using

The other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal

Using the key to multicast data stream decoding receives the multicast data stream.

Can firstly the optical network user end of the optical network line terminal sends multicast application of optical network line

Road terminal to the multicast request processing according to user authority is determined whether to the optical network user

End distributing multicast. If the user does not multicast authority optical network line terminal is not the multicast request

Processing; If the user multicast authority and it is not stored in the multicast when the process of processing such as

Lower:

A1 optical network line terminal to apply for obtaining new data multicast;

A2 optical network line of terminal distribution the multicast occupies a downlink service channel;

A3 is composed of optical network line terminal generates a key and the key as the multicast the Common key;

A4 optical network line terminal uses the other service channel the key is sent to corresponding optical network

Network user terminal;

A5 optical network line terminal uses the distributed uplink service channel as multicast data transmission

Channel to the authority of optical network user terminal opens the downlink service channel the right; A6 optical network line terminals according to key to multicast data stream encrypted and sends authority of

Optical network user terminal according to the key receiving multicast data stream.

If the user multicast authority and it has been stored in the multicast when processing process is as follows:

B1 optical network line terminal uses the other service channel the multicast public key and sends it to The optical network user terminal;

B2 optical network line terminal to the optical network user terminal opens the service channel the right;

B3 optical network user terminal according to multicast public key encryption receiving multicast data stream.

Optical network user end of exiting multicast when the optical network user end of the optical network line the terminal

Sent from the multicast application of optical network line terminal processing the multicast request closing the user the

Of multicast channel of downlink service authority. If it is the last one multicast user the optical network line terminal

End of the upper level network transmitting the multicast application of optical network line terminal stops the from the upper level network to receive

The multicast flow closed the multicast channel using.

Said service channel can be used as the channel number virtual channel identifier or virtual channel identifier

Character identification. Said optical network user terminal can be used as optical network user unit or optical network user terminal.

This invention has the beneficial effect is as follows: By using this invention it only needs to send a part of multicast data stream to

Can realize multicast pon it saves downlink data width. Olt can be used to the multicast user to

Supply better band width capability of each multicast channel has no matter how many subscriber applies it will not affect

Downlink data transmission bandwidth the system can supply more multicast channel to the user at the same time uses.

To multicast data stream encrypted and the key and sends it to user terminal user terminal according to the key

Decrypting which further guarantees the multicast the safety of data is ensured that the user multicast authority

User can receive the multicast data.

Specification attached drawing

Picture 1 is multicast pon network structure conventional diagram;

Picture 2 in existing technology and the multicast copy master to sketch map;

Picture 3 the invention and realizing multicast principle picture;

Drawing 4 the invention applies for multicast flow chart;

Pattern 5 the invention multicast exits the flow pattern.

Specific implementing manner

According to the lower part of the attached drawing and embodiments of this invention is further detailed explain:

Picture 3 represented the invention claims a method for realizing passive optical network method of multicast the multicast

Agent is set on the optical network line terminal olt it is of each user end such as the onu/ont

Multicast request to olt olt sends processing multicast request to the onu/ont transmitting multicast data

Current. A plurality of onu/ont applying the same multicast data stream when olt by using a plurality of service channel

Send only one multicast data stream applying the multicast of onu/ont is to get the multicast data stream Of the received authority so as to realize multicast function.

Can be composed of the olt and generates a plurality of key and the key as the multicast public key the Transmitting multicast data stream when using the key to encrypt; And the key by using the other service through

Channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal by using the key

To the multicast data stream decoding receives the multicast data stream which ensures the multicast authority for

User can receive the multicast data.

Such as drawing 4 the display the invention applies for multicast flow diagram of multicast application it comprises the steps as follows:

1 is formed by the user terminal according to the onu for example to explain to olt sends igmp internet Group management protocol packet requesting multicast;

2 olt processing multicast request according to the user authority is determined whether distributing multicast;

3 if the user does not multicast authority of the olt it is not the multicast request processing;

If the user multicast authority then olt processing multicast;

4 olt processing multicast time if it is not stored in the multicast the processing process is as follows:

1 olt is to apply for obtaining new data generating multicast a multicast address and multicast stream;

2 and the distribution of the multicast occupies a downlink service channel by channel number port id Virtual channel identifier vpi or virtual channel identifier address to identify vci port is id

Gpon data frame structure one of the character of gem frame section is in pon the multi-channel multiplexing service to

Supply service identifier; Vpi/vci for gpon data frame structure frame in the fields of atm;

3 by olt produces a key olt the key as the multicast public key;

4 olt using another service channel by channel number port id of virtual channel identifier

Vpi virtual channel identifier address vci to identify the key is sent to corresponding to the onu

User;

5 olt using the distribution of the downlink service channels as multicast data transmission channel to the

Multicast authority of users open the downlink service channel the right;

6 olt by using the key to multicast data stream encrypted and sends according to the onu

Receiving the key decrypting so as to obtain multicast data.

If it has been stored in the multicast the processing steps are as follows:

1 olt to the user opens the other special service channel the right and using the special service

Channel the multicast public key and sends it to the onu user;

2 olt to the user opens the down multicast service channel the right;

3 onu according to the received key for decrypting so as to obtain multicast data.

Picture 5 which is displayed in the invention multicast exits the flow pattern it comprises the steps as follows:

1 olt to onu sends igmp leave multicast request;

2 and processing the multicast request closing the user the multicast service authority channel;

3 if it is not the last each multicast user the olt it does not carry out any additional processing and so on To the multicast information command processing;

If it is the last one multicast user the olt the superior network sends igmp leave multicast

Group olt stopping request from the upper level network receiving the multicast flow closed multicast channel the use of such as

To the multicast information command processing.

And olt it can not generate key can be composed of the olt directly to the onu/ont sending Multicast data stream. The olt by using a plurality of service channel transmitting a part of multicast data stream by olt

Through management channel or the other channel to the onu distributing multicast receiving authorization only has receiving weight

Limit of onu/ont only can be obtained by the multicast data stream. At the same time this utility model claims an encrypting method is not only

Needs to send one multicast data stream this utility model can realize multicast pon.

By using this invention using the same service channels as same as the port id or vpi/vci of Service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively

For the same multicast of different user transmitting multicast encrypted key. It makes the application of pon network the access

System it reduces the transmission system multicast downlink transmission to the frequency band occupied bandwidth to the olt can be

Multicast user provides better band width capability of each multicast channel has no matter how many user applies

Model are it does not affect the downlink data transmission bandwidth system can supply more multicast channel to the user

At the same time uses. The field of technology of operator does not break away from the essential of this invention and mental can have many variable

Shape of the realization of project this invention is the only the invention is good it can be carried out in the embodiment of the existing is not

So as to limit the invention claims a right range fan through using this invention specification and attached drawing of the content of the equal

The structure change is contained in this invention a right range.

Claims:

1. a method for realizing passive optical network multicast method wherein the: To the multicast receiving the authority a plurality of optical network user terminal optical network line terminal to the same multicast distributing a downlink service channel only parts of sending the multicast data stream; Optical network line the terminal has a broadcast receiving the authority optical network of user end opening of said downlink service channel the right of the optical network user terminal can receive the multicast data stream.
2. According to claim 1 said realize passive optical network multicast method wherein the: Is composed of optical network line terminal generates a key and the key as the multicast public key transmitting the multicast data stream when using the key to encrypt; And the key by using the other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal by using the key to multicast data stream decoding receives the multicast data stream.
3. According to claim 1 or 2 the utility model can realize passive optical network multicast method wherein the: By optical network user end of the optical network line terminal sends multicast application of optical network line terminal to the multicast request processing according to user authority is determined whether to the optical network user terminal distributing multicast.
4. according to claim the realization of the passive optical network multicast method wherein the: If the user does not multicast authority optical network line terminal is not the multicast request processing; If the user multicast authority and it is not stored in the multicast when processing process is as follows: A1 optical network line terminal to apply for obtaining new data multicast; A2 optical network line of terminal distribution the multicast occupies a downlink service channel; A3 is composed of optical network line terminal generates a key and the key as the multicast public key; A4 optical network line terminal uses the other service channel the key sending to corresponding optical network user terminal;

A5 optical network line terminal uses the distribution of the downlink service channels as multicast data transmission channel to the authority of optical network user terminal opens the downlink service channel the right; A6 optical network line terminals according to key to multicast data stream encrypted and sends authority of optical network user terminal according to the key receiving multicast data stream.

5. according to claim 1 said utility model can realize passive optical network multicast method wherein the: If the user multicast authority and it has been stored in the multicast when processing process is as follows: B1 optical network line terminal uses the other service channel the multicast public key and sends it to the optical network user terminal; B2 optical network line terminal to the optical network user terminal opens the service channel the right; B3 optical network user terminal according to multicast public key encryption receiving multicast data stream.

6. according to claim the realization of the passive optical network multicast method wherein the: Optical network user end of exiting multicast when the optical network user end of the optical network line terminal sends the multicast application of optical network line terminal processing the multicast request closing the user the multicast service the downlink channel authorization.

7. according to claim 1 said utility model can realize passive optical network multicast method wherein the: If it is the last one multicast user the optical network line terminal to the superior network transmitting the multicast application optical network line terminal stops the from the upper level network receiving the multicast flow closed the multicast channel using.

8. according to claim the realization of the passive optical network multicast method wherein the: Said service channel is comprised of a channel number virtual channel identifier or virtual channel identifier identifying.

9. according to claim the realization of the passive optical network multicast method wherein the: Said optical network user terminal to the optical network user unit or optical network user terminal.

Chinese Patents Fulltext

© 2013 Scipat Benelux NV. All rights reserved.

Dialog® File Number 325 Accession Number 1981744

Search Notes 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search CPC (H04J3/0655 OR H04N21/6405 ORH04N21/47202 OR H04Q11/0067 ORH04H20/69 OR H04L63/0428 ORH04L63/0435 OR H04L9/08) limited by keywords	2/7/2013	OK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/OLEG KORSAK/ Examiner.Art Unit 2492	
---	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731	
	Filing Date		2011-09-20	
	First Named Inventor	Dezhi ZHANG et al.		
	Art Unit			
	Examiner Name	Unknown		
	Attorney Docket Number		AFD111101435-US	

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1866857	CN	A	2006-11-22	HUAWEI TECHNOLOGIES CO., LTD		☐
	2	1855834	CN	A	2006-11-01	HUAWEI TECHNOLOGIES CO., LTD		☐
	3	2000228668	JP	A	2000-08-15	NEC CORP		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731
	Filing Date		2011-09-20
	First Named Inventor	Dezhi ZHANG et al.	
	Art Unit		
	Examiner Name	Unknown	
	Attorney Docket Number		AFD111101435-US

If you wish to add additional Foreign Patent Document citation information please click the Add button				Add
NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
	1	International Search Report for PCT/CN2010/078611 dated January 21, 2011	☐	
If you wish to add additional non-patent literature document citation information please click the Add button				Add
EXAMINER SIGNATURE				
Examiner Signature	/Oleg Korsak/		Date Considered	02/06/2013
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.				
¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.				

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2011-09-20
First Named Inventor	Dezhi ZHANG et al.
Art Unit	
Examiner Name	Unknown
Attorney Docket Number	AFD111101435-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ling Wu/	Date (YYYY-MM-DD)	2012-01-05
Name/Print	Ling Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /O.K

<i>Index of Claims</i> 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant											☐ CPA											☐ T.D.											☐ R.1.47										
CLAIM			DATE																																								
Final	Original	02/07/2013																																									
	1	✓																																									
	2	✓																																									
	3	✓																																									
	4	✓																																									
	5	✓																																									
	6	✓																																									
	7	✓																																									
	8	✓																																									
	9	✓																																									
	10	✓																																									
	11	✓																																									
	12	✓																																									
	13	✓																																									

PON system multicast authority managing and controlling method**Patent Assignee (name, country):** HUAWEI TECH CO LTD, CN**Inventor (name, country):** ZHAO MING JIANG, CN**Patent Publications**

	Patent Number	Kind	Date	Application Number	Kind	Date		
Main Patent	CN 1866857	A	20061122	CN 200510103487	A	20050919		
H04L-0012/24	A	I	F	B	20060101	20061122	H	CN
H04L-0009/00	A	I	L	B	20060101	20061122	H	CN
H04N-0007/173	A	I		R	20110101	20110101	M	EP

Record Type (Availability): ABSTRACT; SPECIFICATION; CLAIMS ; IMAGE**Word Count:** 2696**Publication Language:** CHINESE**Translation Language:** Human Assisted Machine Translation to English**Abstract:**

The invention relates corresponding to the technical field of PON system multicast jurisdiction control method, device and is a user requesting jurisdiction on OLT, a that receiver the user, OLT distributed of downlink service channel and a common key for user ONT, and timing updating the common downlink service channel and a common key, and is provided with a preview jurisdiction's preview the number of the secondary user of each time preview time and scheduled time, is used to realize to the control of multicast service jurisdiction. The invention realizes control of PON network access system and on-demand playing method, so single wires with the corresponding jurisdiction user to obtain the corresponding service, wherein develop to the commercial the PON system for video on - demand server.

Legal Status Count: 3**Legal Status Information**

Date	Legal Event	Details
20091104	rejection of a patent application for invention after its publication	Effective Date: N/A
20070117	initiative for examination as to substance/operation of substantive examination	Effective Date: N/A

20061122	publication	Effective Date: N/A
----------	-------------	------------------------

Detailed Description:

The PON system multicast jurisdiction control method
technical field

The invention relates corresponding to the technical field, especially to the PON system multicast jurisdiction control method.

background technology

The recent years, along with the popularization rapidly growing and personal computing of Internet, arc of Internet data stream intensified the capacitor constraint of access part; the access network the traditional copper cable access method of to the communication service obviously the demand device. Therefore, overglass wire is gradually widely; the optical fibre is a large in a transmission range wide and capacitor, a voltage, the anti-interference capability water-blocking strong and merits, very further used is high-speed, broadband service transmission method. The light access technologies, PON (passive optical network), due to the passive node, a attachment and for warning and low cost, transparent and easy upgrading and merits is theme to the service pays warning.

PON and emerging broadband access optical fibre technology, comprising no need node equipment and light branching socket, only circuit is a simple optical splitter, and a therefore the economical optical resource and bandwidth resource sharing, economical machine room investment and safety device is high fishing, network speed head and comprehensive fishing network and low cost state power.

At the same time, along with the quick growing communication, a digital multimedia signal more and multiple is further favored by people, realizing video or audio the requesting, and multicast broadcast and applications of through the network access, wherein the fixture with with a later accessing system of.

Shown and a digital 1 is the PON multicast network frame schematic drawing, the passive optical network from OLT (optical network line terminal) accessing signal, (optical distribution network assigns) is ODN to each user terminal ONU/ONT, ONT is an optical network user terminal, is arranged on the user terminal by; The ONU of optical network user device, to the Ethernet is connected with the user premises and network, a watch the multimedia signal of the user terminal. And OLT located between local-side, ONU/ONT is arranged on the user terminal, OLT to the ONU/ONT direction of the lower direction; otherwise of the direction of. The direction of using time division multiplex-based the multicast manner, a ODN methods according to any power-average from the optical signal of OLT to input multiple output user, premises generally 1 are 16 and 1 are 32 or 1 are 64 and allocative decisions. The existing multicast video on - demand operation process reference shown the digital 2, 2 shape is a device for multicast video on - demand of the PON system for accessing method for flow. The position, OLT is multicast each group assigns an independent of downlink service slot; each group multicast is a transmitting multicast data stream, and user of the multicast data stream is a lower terminals and sent for requesting application ONT is screwed on the normally channel. OLT flowing of a common key for multicast each group, while transmitting multicast data stream; and key end of the encryption; And transmitted by the method of the same and service common channel of a multicast receiving jurisdiction ONT, ONT using the same end is the multicast data stream over common channel service the decryption, for receiving and retransmits to a user the multicast data stream.

It is not difficult see to back method and realizes the same PON port users and multiple ONT to send of the requesting wire, OLT according to the allocated on each PON port is a transmitting multicast data relate to realize multi-user of performing requesting the capacitor. Further provided with considered device for managing user to requesting jurisdiction, ONT the process of a user requesting is not control wire, therefore, is to develop the multicast service of each pair must be controlled; and video on - demand server, wherein requirement to each ONT user the requesting jurisdiction of each multicast units and control the OLT respectively, and user lower ONT the condition according is not rod is to develop

the video on - demand server.

Therefore, need to a method for is connected to the requesting end users' jurisdictions end of the control. invention content

The problem of the view of the fact of the existing technology, comprising the volume of this invention is a PON system multicast jurisdiction control method, wherein a user requesting jurisdiction on OLT, a that receiver the user, OLT for user distribution of downlink service channel and a common key, and timing updating the common downlink service channel and a common key, and is provided with a preview jurisdiction's preview the number of the secondary user of each time preview time and scheduled time, is used to realize to the control of multicast service jurisdiction.

An objective of the present invention approves the following technical solution is realized: The invention claims a PON system multicast jurisdiction control method, comprising: A and PON system of optical network line terminal OLT is user requesting; jurisdictionB and user and multicast service processing, OLT is provided with a user distribution of requesting jurisdiction for developing the multicast service multicast group of downlink service channel and a common key, and updating timing. The user requesting jurisdiction is a shaft according to the user the PONID determination of optical network user terminal ONT.

The user jurisdiction is comprises: authorization, non-authorization and/or preview.

The invention claims A - comprising: A1, comprising a step number of the timing time preview and/or a preview value of the position limit of scheduled time preview.

The pedal B comprises: B1 and the user with a preview jurisdiction, and preview time and/or scheduled time preview value of times of a specified upper limit; B2 and OLT wherein the common downlink service channel and a common key.

The pedal B1 comprises: B11 and according to of the user requesting jurisdiction for determining of the user for user receiver.

The pedal B comprises: Starting timing a distribution of downlink service channel and a common key, achieves the scheduled time to updating to the common downlink service channel of every time.

The pedal B comprises: Starting timing a distribution of downlink service channel and a common key, achieves the scheduled time to updating to the key of every time.

- Comprising:

Determines the user for non-authorized user, and OLT terminates requesting application processing to the user.

A see of the present invention provides's technical solution of the invention realizes the control of PON network access system and on-demand playing jurisdiction, is divided into the authorization, the non-authorization preview and user requesting jurisdiction, so single wires with the corresponding jurisdiction user to obtain the corresponding service, and enables with a preview jurisdiction user - time preview program flow, wherein develop to the commercial the PON system for video on - demand server.

Brief description for drawings

Digital 1) is an existing PON multicast network frame schematic drawing; Digital 2 is the existing PON network access system based on multicast video on - demand the operation flow, imageDigital 3 is the invention PON access system for realizing user on-demand playing control jurisdiction operation current map.

detailed description of illustrated embodiments

The core in of this invention is to provide the PON system multicast jurisdiction control method, wherein a user requesting jurisdiction on OLT, a a receiver, user OLT for user distribution of downlink service channel and a common key, and timing updating, and is provided with a preview jurisdiction's preview the number of the secondary user of each time preview time and scheduled time, is used to realize to the control of multicast service jurisdiction.

The invention claims a PON system multicast jurisdiction control method, is referred to shown the digital 3 is the invention claims a method for operating current position, the PON system multicast jurisdiction control method exactly comprises: Steps: 10 OLT receiving and processing ONT the

requesting request the user; The user of the interconnection system of area networks managing protocol) protocol sending the requesting request through; IGMPSteps: 11 OLT time authentication to the user; Capable of the user requesting jurisdictions the OLT for pre-twisted patching bar; each and user in aggregate of the user jurisdiction table of each group multicast, according to the users' ONT PONID stipulated of the user the requesting jurisdictions; the user jurisdiction table stipulated the user the requesting jurisdiction is includes: The authorization and non-authorization, a preview and ranks, and is capable user of each time preview time and/or a preview value of the position limit of scheduled time, preview

OLT after receiving user requesting request, and user ONT PONID, compares the user jurisdiction table to determine the user according to the PONID the requesting; jurisdictionSteps: 12And the user has been receiver or with a preview jurisdiction, and search OLT local the information in whether a group multicast data stream of the user request; OLT according to the user requesting request search information local set in with the user request the group multicast data stream; The local information module is used to save the local group multicast data stream; informationSteps: 13Each of the group multicast data stream; and OLT obtaining the group multicast data stream to the upstream device, applicationEach OLT is not made of the user request to the local information in the group multicast data stream; and OLT obtaining the group multicast data stream to the upstream device, applicationThe upstream device is connected to obtain the group multicast data stream a routing server and broadband access server the network device; Steps: 14 OLT of the group multicast data stream assigns a new of downlink service channel number and new public key, and starting timing, wherein the output of downlink service channel and a key, overtimeThe gaining the group multicast data stream of the user request, OLT of the group multicast data stream assigns a new of downlink service channel number and new public key, a OLT generating the novel of downlink service channel number and a starting timing, wherein of the output current of downlink service channel value and a overtime, achieves the scheduled time to updating the common downlink service channel are respectively and each key time, namely OLT timing replaces the common downlink service channel and a common key; the scheduled time of value according to the circuit; andIn turn to realize simply; the exchanging operation can only be of the key, a maintaining of downlink service channel are provided; invariableSteps: 15 OLT transmitting device for encrypting multicast data stream over common downlink service channel of the; anThe OLT completes the operation, transmitting the user request over common downlink service channel of the assignment for multicast data set, and encryption to the group multicast data stream by the novel public key of the; anAnd the step 12, search OLT the user request to the local information in the group multicast data stream, which directly and step 15, operationsSteps: 16The operation completes, wherein from user with preview; jurisdiction

Steps: 17And the user with preview jurisdiction, a judging preview time and preview value of the secondary, whichAnd the user with preview jurisdiction, according to the preview time and scheduled time according the preview time and/or a preview value of times of preview value of times of each user in the user jurisdiction table stipulated, whichSteps: 18And the output is preview time and/or a preview the position of, while the OLT scram the transmitting multicast group data stream to the user ONT the common downlink service channel and a key; When the output is preview time and/or a preview value of times the appointed time, OLT periphery of the transmitting multicast group data stream to the user ONT the common downlink service channel and a key, the user preview operation is forbidden; Steps: 19And the user there is no preview jurisdiction, wherein the user jurisdiction is a authorization, or the preview time and preview value of times of the output user is not the specified upper limit, and OLT through a a channel transmission the common downlink service channel and a key of multicast set of user ONT; And a plurality of the group multicast data stream of the user request associated with the novel of downlink service transmission channel of OLT distribution, the user ONT without and obtaining the common downlink service channel of key and a receiving the group multicast data stream; informationSteps: 20A step is 11 from user for non-authorized user, and OLT terminates requesting application processing to the user.

The summary, the invention realizes control of PON network access system and on-demand playing

method, so single wires with the corresponding jurisdiction user to obtain the corresponding service, wherein develop to the commercial the PON system for video on - demand server.

The is of the only the invention good detailed description of illustrated embodiments, and has a protection of this invention are not to limit, a provide of any of familiar and technical field in a range of the invention exposition, the exchanger or the alternative capable of think easily, and covered on the has a protection of this invention. Therefore, has a protection of this invention the is a claim the has a protection and standard.

Claims:

1. 1 PON system multicast jurisdiction control method, comprising a characterised, comprising: A and PON system of optical network line terminal OLT is user requesting; jurisdictionB and user and multicast service processing, OLT is provided with a user distribution of requesting jurisdiction for developing the multicast service multicast group of downlink service channel and a common key, and updating timing.
2. The user requesting jurisdiction of PON system multicast jurisdiction control method according to claim 1, comprising a characterised, wherein a shaft according to the user the PONID determination of optical network user terminal ONT.
3. The user jurisdiction of PON system multicast jurisdiction control method according to claim 1 or 2, characterised is composed, comprising: authorization, non-authorization and/or preview.
4. PON system multicast jurisdiction control method according to claim 3, characterised is composed, wherein the invention claims A - comprising: A1, comprising a step number of the timing time preview and/or a preview value of the position limit of scheduled time preview.
5. The PON system multicast jurisdiction control method according to claim 4, wherein the is composed characterised, wherein the B comprises: B1 and the user with a preview jurisdiction, and a preview time and/or scheduled time preview value of times of a specified upper limit; B2 and OLT wherein the common downlink service channel and a common key.
6. The PON system multicast jurisdiction control method according to claim 5, wherein the is composed characterised, wherein the B1 comprises: B11 and according to of the user requesting jurisdiction for determining of the user for user receiver.
7. The PON system multicast jurisdiction control method according to claim 1, wherein the is composed characterised, wherein the B comprises: Starting timing a distribution of downlink service channel and a common key, achieves the scheduled time to updating to the common downlink service channel of every time.
8. The PON system multicast jurisdiction control method according to claim 1, wherein the is composed characterised, wherein the B comprises: Starting timing a distribution of downlink service channel and a common key, achieves the scheduled time to updating to the key of every time.
9. PON system multicast jurisdiction control method according to claim 1, comprising a characterised, further - comprising: Determines the user for non-authorized user, and OLT terminates requesting application processing to the user.

Chinese Patents Fulltext

© 2013 Scipat Benelux NV. All rights reserved.

Dialog® File Number 325 Accession Number 1992767

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4909	passive optical network	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
L2	790	L1 AND key	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
L3	323	L2 AND encrypt\$3	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
L4	101	L3 AND (optical line terminal)	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:19
L5	30	L4 AND multicast	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:19
L6	30	L5 AND tim\$4	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:20
L7	10	L6 AND downlink	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:21
L8	16943	((H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08).CPC.)	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:24
L9	1130	L8 AND L1	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:25
L10	14	L8 AND L6	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:25

EAST Search History (Interference)

<This search history is empty>

2/ 7/ 2013 7:42:35 AM
C:\ Users\ okorsak\ Documents\ e-Red Folder\ 13257731 Zhang\ 13257731 Zhang.wsp

Notice of References Cited	Application/Control No. 13/257,731		Applicant(s)/Patent Under Reexamination ZHANG ET AL.	
	Examiner OLEG KORSAK		Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0136372 A1	07-2004	Gruia, Dumitru	370/390
*	B	US-7,301,968 B2	11-2007	Haran et al.	370/508
*	C	US-2008/0155255 A1	06-2008	Ohira et al.	713/160
*	D	US-2010/0174901 A1	07-2010	KHERMOSH et al.	713/160
*	E	US-2010/0239252 A1	09-2010	Davis et al.	398/58
*	F	US-2011/0029773 A1	02-2011	Effenberger, Frank J.	713/168
*	G	US-2012/0128155 A1	05-2012	Effenberger, Frank J.	380/256
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	CN1855834	10-2006	China	He	380/256
	O	CN1866857	10-2006	China	Jiang	380/256
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2012-01-06
First Named Inventor	Dezhi Zhang et al.
Art Unit	2492
Examiner Name	KORSAK, OLEG
Attorney Docket Number	AFD111101435-US

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20060031936	A1	2006-02-09	Enterasys Networks, Inc.			
	2	20070133800	A1	2007-06-14	Electronics & Telecommunications Research Institute			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	101547086	CN	A	2009-09-30	HUAWEI TECHNOLOGIES CO., LTD.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731
	Filing Date		2012-01-06
	First Named Inventor	Dezhi Zhang et al.	
	Art Unit	2492	
	Examiner Name	KORSAK, OLEG	
	Attorney Docket Number	AFD111101435-US	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	CN101547086A; Automatically Translated by the Intellectual Property Publishing House of SIPO, March 21, 2013 see pages 1-12	☐
	2	XP11382244, ON EPON SECURITY ISSUES; The Electronic Magazine of Original Peer-Reviewed Survey Articles;1ST QUARTER 2007, VOLUME 9, NO.1; pages 68-83.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2012-01-06
First Named Inventor	Dezhi Zhang et al.
Art Unit	2492
Examiner Name	KORSAK, OLEG
Attorney Docket Number	AFD111101435-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ling Wu/	Date (YYYY-MM-DD)	2013-04-26
Name/Print	Ling Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	15618853
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	26-APR-2013
Filing Date:	20-SEP-2011
Time Stamp:	10:08:13
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	CN101547086A.pdf	1238206 93603676823eb0af609b182539b9005d3fb7d364	no	26

Warnings:

Information:

2	Foreign Reference	CN101547086A_translation.pdf	1669511	no	12
			32d74be6894feb5f1f49f89842523e7a8dca4e92		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Foreign Reference	On_EPON_Security_issues.pdf	3433848	no	16
			6832d37e3b3fab6688edd4485249c5e1883728c		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Foreign Reference	US2006031936A1.pdf	2841802	no	14
			6964dcfbce0ec7ce8263def8725ad4d7d8965037		
Warnings:					
Information:					
5	Foreign Reference	US2007133800A1.pdf	3059543	no	18
			d7d17e4167a830df53ad966ab40e365a91c141d2		
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	Supplemental_IDS_AFD111101435-US.pdf	612645	no	4
			c431601507b3205d22a030a5ca39447027655b21		
Warnings:					
Information:					
Total Files Size (in bytes):			12855555		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CN101547086 A 20090930

Automatically Translated by the Intellectual Property Publishing House of SIPO

Embodiment of this invention has disclosed sowing control system, method and apparatus in a broadband group of access network, this system includes: Insert the control subsystem, is used for producing the group and sowing and encrypting the key word, sow the stated group to encrypt the key word to send to user's subsystem, and after the subscription receiving user's subsystem and sending is asked, utilize the stated group to sow and encrypt the key word and sow frames to encrypt the group to user's subsystem, sow the stated group that has encrypted the frame to send to the stated user's subsystem; User subsystem, use for to insert control subsystem, send, subscribe, ask, come, ask group sow frame while being stated, sow, encrypt key word stated access group that controlate subsystem encrypted that decipherment receive, sow frames according to access group that controlate subsystem send that receive. This invention insert employ, authorize user use group sow business datum in broadcast type (share medium), prevent the disabled user from using the group to sow the business, sow the safety that the authority controls after strengthening the group.

A broadband group of access network sows control method, system and device

Technical field

This invention involves the technical field of communication, especially involve sowing control method, system and device in a broadband group of access network..

Prior art

As network being broad band progressively, the new businesses is emerging constantly, especially IPTV (Internet TV) a kind of business gets a large amount of application. Because generally the group sows (sow more) the application mode in IPTV business, namely share with a copy of data many people at the same time, such as not watching the same television channel / program with users, this can not bring the difficulty to authority management of the network littly.

In users, generally carrying on the group sows the authority and controls in DSL (Digital Subscriber Line, Digital Subscriber Line) in the marginal group of network sow the authenticating device, the group sows the authenticating device and includes inserting the node (AccessNode,AN), generally sow the group setting up users in the authenticating device in the group and sow the control table of the authority, for example: The group sows and visits the control table (Access Control List, ACL). Group broadcast authenticating device broadcast authority controlate table, control user broadcast the visit of the channel to the group through group, because DSL usually clicks to and clicks inserting (namely: The route that is connected is monopolized), broadcast the control table of the authority and control users to broadcast the visit of the channel to the group effectively through the group, insert for person who broadcast (share medium), group sow it flows to be whom radio (sow more) send, namely a user has asked for a group to sow and flow, the users in this radio land can receive this group to sow and flow.

The broadcasting type (share mediums) mainly inserts including PON (Passive Optical Network, there is no source light network), WIMAX (Worldwide Interoperability for Microwave Access, global microwave interaction is inserted),etc.. For example: A user under interface of one PON watches a program channel, the group that all users can receive this program in interface of this PON broadcasts and flows, namely all users in this PON can watch this program, the point symetry multipoint transfer characteristic that broadcasts because of the group, the group sows members and shares the group to sow and flow, so can't adopt point-to-point encryption.

Carry on the group and sow the authority to control in the prior art systematically through CA (CA Conditional Access) broadcasting the television system, main application is in the field of broadcast and television, such as the digital television field, CA system which broadcasts the television system mainly encrypts the application layer in the head end system, then carry on CA Conditional Access through the roof box (STB).

In the prior art, authorize central control on the head end, system implementation is complicated, it is apt to cause the characteristic bottleneck; The roof box embeded with intelligent card of general requirement, are unfavorable to the operators media's content shares; And it is unsuitable in the network application of broadband to broadcast CA system of the television system.

Invention content

Embodiment of this invention has offered a broadband group of access network to sow control method, system and device, the legal group sows member's users and uses the group to sow the business datum, prevent the disabled user from using the group to sow the business.

Embodiment of this invention has offered the group of access network of a kind of broadband to sow the control system, including:

Insert the control subsystem, is used for producing the group and sowing and encrypting the key word, sow the stated group to encrypt the key word to send to user's subsystem, and after the subscription receiving user's subsystem and sending is asked, utilize the stated group to sow and encrypt the key word and sow frames to encrypt the group to user's subsystem, sow the stated group that has encrypted the frame to send to the stated user's subsystem;

User subsystem, use for to insert control subsystem, send, subscribe, ask, come, ask group sow frame while being stated, sow, encrypt key word stated access group that controlate subsystem encrypted that decipherment receive, sow frames according to access group that controlate subsystem send that receive.

Embodiment of this invention has offered a broadband group of access network to sow the control method, including the following steps:

Produce, combine distribution group, sow, encrypt key word set, stated group sow, encrypt key word set, include at least one group sow, encrypt key word and correspondent group, sow, shed marking;

Receive it after subscribing and asking, utilize the stated group to sow and encrypt the key word and sow frames to encrypt the group;

Sending the stated group that has encrypted sows frames, the stated group that has encrypted sows frames and sows and encrypts the key word to carry on decipherment with the stated group.

A kind of access controlling device of embodiment of this invention, comprising:

The key word produces the unit, used for producing the group and sowing and encrypting the set of the key word, the stated group sows and encrypts the set of the key word to include the at least one group sows and encrypts key word and correspondent group to sow and flow markings;

Key word distribute unit, use for, send stated key word, turn into group that Entrance turn into, sow and encrypt the key word to user subsystem;

Die Datenannahme unit, use for, receive, come from group sow source group of apparatus, sow frames and group from user's subsystem and sow and subscribe request, and sow the stated group the frame to send the data encryption unit to;

Data encryption unit, are used for sowing and subscribing the group that analyzes out while asking to sow and flow markings from the group, sow, flow marking turn into group of unit, sow, encrypt key word, obtain group, sow, encrypt key word in the set from stated key word according to stated group, turn into group that unit turn into, sow, encrypt key word and correspondent cryptographic algorithm, sow frame, pay, encrypt with stated key word to to user's subsystem group, and sow the group encrypted the frame to send to the data to send the unit;

The data send the unit, is used for confirming the stated die Datenannahme unit is received after the subscription that user's subsystem send is asked, until group sow, transfer to, publish to user subsystem sending stated data encryption group that Entrance encrypted, sowing frames.

Embodiment of this invention hits, inserts in the radio type (share mediums) while employing, authorize users to use the group to sow the business datum, prevent the disabled user from using the business. Sow emergency control after strengthening the group sharing mediums and inserting, has stopped not to authorize or visit maliciously, have protected the investment of the operator.

Illustration

Fig. 1 is that embodiment of this invention hits the group of access network of broadband and sows the control system;

Fig. 2 is the application schematic view in PON system in embodiment of this invention;

Fig. 3 is that the group sows the business and controls the flow chart in embodiment of this invention;

Fig. 4 is that the key word that embodiment of this invention hits PON system break or switch over the flow chart;

Fig. 5 is the daily application flow chart which shares the medium system in embodiment of this invention;

The cleartext group before Fig. 6 encrypts in embodiment of this invention sows the frame schematic view;

The group after Fig. 7 encrypts in embodiment of this invention sows the frame schematic view;

Fig. 8 is that gigabit has no network frame structure of source light in embodiment of this invention;

Fig. 9 is that gigabit has no network key word news structure of source light in embodiment of this invention;

Fig. 10 is that it have no network key word news structure of source light that embodiment of this invention hits Ethernet.

Concrete embodiment

Have offered the group of access network of a kind of broadband to sow the control system in embodiment of this invention, can apply to PON or and share dailily in systems such as mediums,etc., as shown in Fig. 1, comprising: Insert control subsystem 100 and user's subsystem 101, 102, 103. Wherein,

Insert control subsystem 100 to include: The key word produces the unit (Key Generator Unit, KGU) A101, key word are distributed the unit (Key Distribution Unit, KDU) A102, controlling authorizing the unit (Control Authorization Unit, CAU) A103, data encryption unit (Data Encryption Unit, DEU) A104, data send the unit (Data Sending Unit, DSU) A105, subscribing management unit (Subscription Control Unit, SCU) A106, die Datenannahme unit (Data Receiving Unit, DRU) A107;

User's subsystem includes separately: Terminal to subscribe the unit (Client Subscription Unit, CSU) B101, terminal decipherment unit (Client Decryption Unit, CDU) B102, terminal key word unit (ClientKey Unit, CKU) B103.

Inserting control subsystem 100 can be realized in an apparatus, the stated apparatus includes: DSLAM(Digital Subscriber Line Access Multiplexer, inserting multiple connection device of the Digital Subscriber Line), NAS (Network Access Server, the server of access to networks), edge router, base station,etc., also can be that many apparatuses make up (different units are distributed on different apparatuses); CSU B101, CDU B102 and CKU B103 can be distributed in different user terminals, CDU B102 and CKU B103 generally integrate in an apparatus.

Wherein, KGU A101, used for producing the group and sowing and encrypting the set of the key word (Multicast EncryptionKey, MEK), including sowing and encrypting the key word in one or more of groups in this set, these groups sow and encrypt key word and group to sow and flow markings to correspond to, MEK is used for sowing frames and encrypting decipherment to the group.Encryption and decipherment key word that the group sows the frame generally use the symmetrical key word, the length and type, according to realizing the decision of the key word (or call it the cryptographic key) specifically, DEU A104 sow frame, go on, encrypt to group with MEK, user CDUB102 of subsystem broadcast frames, go on decipherment with MEK to group after the encryption, KGU A101 generally produces a random number, and then produce MEK according to this random number through the pseudo-random function (pseudo-random function, PRF).

KDU A102, are used for managing MEK, includes maintaining the state of MEK, distributing MEK, notifying user that the subsystem break or switch over MEK etc. to user's subsystem, for example: KDU A102 distributes MEK or KDU A102 and informs users of CKU B103 of a subsystem to switch over MEK to CKU B103 of user's subsystem.It can be according to realizing the decision to distribute MEK and and break and switch over the realization agreement that MEK notifies news specifically, can include: OMCI, IGMP, MLD, CAPWAP, MPCP (Multi-Point ControlProtocol, control protocol of the multipoint), OAM (Operations Administration and Maintenance, operate maintenance management), MEK can use, insert control subsystem and user point-to-point key word that subsystem consult in advance, distribute encrypt, the point-to-point key word of what the stated thing is consulted first includes: Point-to-point key word, user's subsystem sharing (pre-shared) in advance notify to the public point-to-point key word (public-key) which insert the control subsystem etc..Sow (or sow more) in the group while employing, one or more of groups sow and flow to share one MEK, all subsystems of legal user (organize and sow members) use decipherment group MEK to sow frames. KDU A102 manages MEK that is safeguarded and is shown in Table 1:

Table 1 MEK state table

[image]

Wherein 227.100.1.0/24 represent the range, represent all groups of markings of sowing flowing of 227.100.1.0 to 227.100.1.255.

CAU A103, used for asking to carry on authenticating to the subscription of user's subsystem, for example: Sow the group to using of control table of the authority to sow and ask to control through the group, the group sows the authority and controls Table 2 to be shown:

Table 2 group sows the control table of the authority

[image]

Group sow authority controlate table dispose in advance generally, sow authority controlate table, can confirm one user visit one group sow, flow and a plurality of group sow authority that flow through group.

DEUA104, used for encrypting the group and sowing frames, the stated group sows frames to mean the group to user's subsystem sows frames, the encryption method (algorithm) that DEU A104 adopts can depend on concrete realization, such as using IPsec encrypting, IEEE (Institute of Electrical and Electronics Engineers, electric and the electronics engineer learns) MACSec of 802.1ae encrypts, the PON layer encrypts, wireless empty mouth encrypting, SRTP (SecureReal-time Transport Protocol, the agreement of failing spreads in real time safely) to encrypt etc..

DSU A105, used for sending the data, including sowing frame, MEK and distributing or switching over news etc. in the group after DEU A104 encrypts.

SCU A106, used in the treated group and sow and subscribe asking, IGMP or MLD report news that CSU B101 substantially as processing user's subsystem sends, SCU A106 can be that one IGMP/MLD survey (snooping) or agent (Proxy) specifically.

DRU A107, used in the receiving data, including receiving and coming from the group that the group sows the source apparatus and sowing frames, group from user's subsystem and sowing and subscribing asking etc..

Embodiment's application of this invention in PON system is shown as in Fig. 2: PON is mounted on the light road to the console for centralized control is terminal (Optical Line Terminals, OLT), only mixing the wire mesh (Optical DistributionNetwork, ODN) and installs in mere network unit (Optical Network Unit, ONU) three parts of user's position and makes up. Transmit the data frame in the downstream direction by the way of broadcasting, the up direction adopts the way of multiplexing to finish the access of a plurality of ONU. It is OLT apparatus to insert control subsystem 100, user's subsystem 101, 102, 103 is ONU (ONT) apparatus and/or host computer. CDU B102 and CKU B103 locate in ONT, CSU B101 can be realized in ONT or host computer. KGU A101, KDU A102, CAU A103, DEU A104, DSU A105, SCU A106, DRU A107 realize in OLT. Now describe that inserts the treatment of control subsystem 100 and user's subsystem.

The treatment which inserts control subsystem 100 includes processing treatment and data of control surface, wherein process including the data:

Insert, receive group, sow group that source send, sow, flow by 100 control subsystem (Multicast Flow, MCFlow), organize and broadcast data flow to go on and encrypt, then sow encrypting the back group and flow and transmit it to user's subsystem, need to prove, as to interface of one PON, inserting control subsystem 100 sends one or many groups to sow and flow, because PON belong to broadcast transmission, so all user subsystem can receive, insert group that control subsystem send, sow and flow. Concrete realization can be: DRU A107 receive group sow group that source send, sow group flow, sow behind the frame, DRU A107 will organize and sow frames to encrypt for DEU A104, DEU A104 sows and flows markings and obtains the group and sows MEK that frames encrypted according to the group that the group sows the frame, then sow frames to encrypt the group according to correspondent cryptographic algorithm and MEK, DEU A104 sow frame, give DSU A105 group encrypt, DSUA105 sow, transfer to, issue, organize, sow frame, transmit, go out according to group, group sow transfer to, issue, set up and delete from SCU A106 generally, group sow transfer to, deliver including the marking sheds and transmit the outlet port (for example: Port), the purpose (organize and sow) of stated flowing IP or Ethernet prelude that the marking can sow the frame from the group is obtained in the address field.

The control surface treatment which inserts control subsystem 100 includes:

Inserting control subsystem 100 receives the group and broadcasts and subscribes asking, analyzing stated subscription asks to obtain the group and broadcast and flow markings, etc. and subscribe the parameter and user identification information, then sow and flow markings and obtain this group and sow and flow marking correspondent MEK according to the stated group, then distribute, get initiate this, subscribe user subsystem that ask MEK this, set up group, sow, transfer to, publish and broadcast members, combine their states of the record as group user subsystem at the same time. Preferred, inserting control subsystem 100 receives and also includes subscribing and asking to process authenticating to this after subscribing and asking, if authenticating fails, does not distribute MEK. Concrete realization can be: DRU A107 receives after subscribing request news, DRU A107 processes this news for SCU A106, SCU A106 analyzes this news, obtain and subscribe parameter and user identification information, CAU A103 processes authenticating according to subscription parameters and user identification information that SCU A106 offer, SCU A106 tells KDU A102 to distribute MEK. KDU A102 inspection group sow flow MEK of marking exist already, if ask KGU A101 and turn into a new MEK without having at first.

Inserting control subsystem 100 receives the group and sows and subscribes withdrawing, inserting control subsystem 100 can break or switch over this and subscribe group withdrawn and included and sow and flow marking correspondent MEK. Inserting control subsystem 100 can support periodic breaking MEK. It can to break MEK be that KDU A102 ask for KGU A101 and produce a new MEK, then keep MEK, distribute agreement news MEK through MEK to send to user's subsystem at the same time.

The treatment of user's subsystem includes processing treatment and data of control surface, wherein process including the data:

User's subsystem receives the group after inserting the encryption that control subsystem 100 sends and sows frames, sow group of frame, sow, flow marking obtain correspondent MEK, then use MEK decipherment stated group encrypt, sow frame according to stated group, CDU B102 realizing specifically that can be user's subsystem sows and flows markings according to the group, obtain MEK from CKU B103.

The control surface treatment of user's subsystem includes:

User's subsystem receives MEK inserting control subsystem 100 and sending and distributes news or switches over news, CKU B103 keeps MEK or and switches over MEK according to this news. User's subsystem can support to sow the group in flowing and sow switching over markings and switching over MEK of the frame according to the group, also can switch over regularly according to time.

User to insert, send, subscribe, ask or withdraw news by 100 controlate subsystem subsystem, notify and insert control subsystem 100 to subscribe or withdraw.

Embodiment's treatment of this invention in PON system is shown as in Fig. 3, it is OLT apparatus to insert control subsystem 100, user's subsystem is ONU (ONT) apparatus and/or host computer, mainly include the following steps:

S301, user's subsystem organizes and sows and subscribes asking at the beginning, for example: Host computer send join, ask, such as specifically: CSU B101 of the host computer sends IGMP or MLD report news, subscribing be able to include subscribing the parameter, user identification information, etc. to ask, the information of the user identification includes IP address, MAC address, terminal marking of the host computer, etc. specifically. Subscribe the parameter including the group sows and flows markings, for example: The group sows the group address.

S302, inserts the control subsystem to subscribe and ask. DRU A107 of OLT receives and joins request news, is transferred to SCU A106 to treat and subscribe and ask, report news such as analyzing IGMP or MLD, obtain and subscribe parameter and user identification information, the message of the user identification can also include OLT receives stated OLT apparatus port which adds request news, CSU B101 tells CAU A103 to ask to carry on authenticating to the subscription of user's subsystem, if authenticating succeeds, tell KDU A102 to distribute MEK to the user terminal, SCU A106 dispose group sow, rotate, publish at the same time, sow member, increase, get group sow member state record, user user identification of subsystem as group. The authenticating of CAU A103 includes specifically: CAU A103 subscription parameter and user identification information according to user, the group which checks users broadcasts the control table of the authority, if the group sows ACL table, the group that users subscribed sows and flows the correspondent authority of the marking in order to allow, then authenticating succeeds.

S303, OLT distributes MEK. Marking of the apparatus that KDU A102 of OLT sent this user subsystem correspondent CKU B103 subscribing and asking it according to the information acquisition of the user identification, MAC address or LLID (logical link marking) such as ONU marking (ID) or GEM PORT information or ONU, KDU A102 of OLT distributes agreement news MEK through MEK to send to user's subsystem. OLT can distributes agreement news and pays and encrypts MEK or MEK through the point-to-point key word. MEK can include the group sows and flows the marking, cryptographic algorithm, can further include the time stamp (timestamp) to distribute agreement news. For example: OLT adopts OMCI to distribute MEK, KDU A102 regards MEK as ME of OMCI (ManageEntity, manage entity) seal, put OMCI into in the news, send OMCI set up news (OMCI message class in the news encode into 8) get to designated ONU, can define one in OMCI and sow more key word ME (Multicast key info)s specifically, sow more key words ME and correspond to a type to number (classvalue, correspondent to Message Identifier the top two), sow more key words ME to include the group sows and flows marking, MEK value, encrypts the type. The group sows and flows markings and organizes the marking which sows the frame correspondingly, it can be that a group sow address, a time stamp or port marking (PORTID).

S304, user's subsystem accepts MEK. ONU receives MEK to distribute agreement news, analyzing this news obtains MEK, then store MEK and correspondent information, for example: The group sows and flows markings, encrypts the type, time stamp, etc..

S305, inserting the control subsystem encrypts the group to sow and flow. DEU A104 of OLT encrypts the group that DRU A107 receives and sows frames, DRU A107 receives the upstream apparatus (for example: IP edge apparatus) group that send sow frame, group that obtain sow group of frame, sow, shed marking, sow and flow markings and obtain MEK according to the group, DEU A104 cryptographic algorithm (type) can be reached an agreement on, in this embodiment, DEU A104 realizes algorithms such as AES of PON, etc. encrypt ATM, GEM frame or load of data (payload) some of the Ethernet frame.

S306, inserting the control subsystem transmits the group and sows frames. DSU A105 of OLT sow frame, send, go out to user subsystem group encrypt, DSU A105 sows and transfers to and issues and transmits the group after encrypting to sow frames according to the group that SCU A106 disposes, namely DSU A105 organize, sow frame, mail to, have PON port of user's subsystem (group broadcast members) only.

S307, user's subsystem decipherment group sows frames. The group received in CDU B102 MEK decipherment according to CKU B103 of ONU sows frames, then sow the group after decipherment the frame to mail to the host computer.

In embodiment two of this invention, MEK of PON system breaks or switches over the application drawing, it is OLT apparatus to insert control subsystem 100, user's subsystem 101, 102, 103 is ONU (ONT apparatus and/or host computer, OLT apparatus uses MEK to distribute or switch over agreement news and notify ONU/ONT. The procedure is shown as in Fig. 4, mainly include the following steps:

S401, inserts the control subsystem to find MEK breaks or switches over the incident, touches off MEK to break or switch over. KDU A102 of OLT measures MEK and switches over the incident, MEK break or switch over incident, include timing (period) touch off, break or switch over incident, insert, receive, subscribe, withdraw by control subsystem 100 (for example: It is touched off that the group sows members and leaves) (such as IGMP that SCU A106 receives users leaves news).

S402, inserting the control subsystem breaks or switches over MEK. KDU A102 of OLT detects MEK breaks or switches over the incident, begin MEK break or switch over and KDU A102 of OLT can break or switch over one or more of group, sow MEK that shed while being disposable, KDU A102 of OLT tells KGU A101 to produce one or more of MEK, then KDU A102 obtains MEK that KGU A101 produced, KDU A102 of OLT inquires of SCU A106 and waits to break or switch over the group of MEK and sow member's state record, KDU A102 and group sow flow marking or switch over mark, seal, put MEK into, distribute or switch over agreement news new MEK, then use MEK to distribute or switch over agreement news and sow members and record to the subsystem members of user of China and notify new MEK or switch over MEK to the group. Stated switching over marks and including time or frame mark, are used for pointing out CDU B102 of user's subsystem launches new MEK and carries on the decipherment group and sows frames, for example: That in ultra frame (Ident) in GPON system replies frame counter value.

S403, user's subsystem switches over or breaks and processes MEK. ONU receives MEK and distributes or switches over agreement news (for example: OAM news), analyzes this news, obtain new MEK or switch over switching over marks of MEK, then store new MEK or switch over switching over marks of MEK.

S404, inserting the control subsystem uses new MEK to encrypt the group and sow frames. DEU A104 of OLT switches over to new MEK and encrypts the group and sows frames, for example: Use new MEK to encrypt the group that DRUA107 receives and sow frames in designated time.

S405, inserting the control subsystem transmits the group after encrypting and sows frames. DSU A105 of OLT sow frame, send, go out to user subsystem group encrypt.

S406, user's subsystem uses new decipherment group MEK to sow frames. For example: CDU B102 of ONU use new MEK group that decipherment receive sow frame in the CKU B103, then broadcast frames, mail group after the decipherment to the host computer in designated time.

Embodiment three of this invention, shares the application drawing of the medium system dailily, it is the accession equipment to insert control subsystem 100, such as DSLAM or IP edge apparatus, user's subsystem 101, 102, 103 is RG and/or host computer, DSLAM or IP edge apparatus and RG support IPSec encrypting or MACSec encrypting or SRTP, the group sows flowing to realize IPSec encrypting or MACSec encrypting or SRTP encrypts, can only need to use ESP when IPSec encrypts, there are no limitations on MEK distributes or switches over the realization agreement of news, for example: SNMP agreement or CAPWAP (Control And Provisioning of Wireless Access Points, wireless to visit point control and dispose the agreement) or TR-069 or IKE. The procedure is shown as in Fig. 5, comprising the steps of:

S501, DSU A105 of IP edge apparatus or DSLAM receives and subscribes asking, begins to process and subscribe asking (for example: Tell KDU A102 to distribute MEK to the user terminal, SCU A106 disposes the group to sow and rotate and issue at the same time, the record group sows member's state). Stated subscription may come from and employ the server (for example to ask: AAA server or tactics control device or network management server) transit shipment, the subscription that DSU A105 of IP edge apparatus or DSLAM receives was asked because through employing transit shipment of the server, so needn't need to continue it to subscribing and asking to carry on authenticating, subscribing can include to ask the group released broadcasts and flows marking and user identification information, the group broadcasts and flows markings including the group broadcasts the group address, the information of the user identification includes the addresses of ports, terminal or host computer, etc.. IP edge apparatus or DSLAM can not possess the authenticating function without CAU A103 and at this moment.

S502, KDU A102 of IP edge apparatus or DSLAM distributes MEK, notify, give user subsystem namely MEK, IP edge apparatus or KDU A102 of DSLAM broadcast, flow marking, etc. MEK or group information seal put into MEK, distribute in the news, send this news to user's subsystem. Group sow flow marking include group sow group IP address, group sow MAC address, SPI, etc., KDU A102 distribute MEK take the exit passageway generally, KDU A102 uses the point-to-point key word to encrypt MEK or MEK to just send out after dividing law news.

S503, accepts MEK. MEK that RG receives KDU A102 of IP edge apparatus or DSLAM divides law news, obtaining MEK transfers to CKU B103 to treat, for example: Keep MEK information.

S504, DEU A104 of IP edge apparatus or DSLAM encrypts the group and sows a group of frames, for example: DEU A104 of IP edge apparatus or DSLAM can use ESP of IPSec to encrypt, also can use MACSec to encrypt, the preferred one uses ESP of IPSec to encrypt, encrypting MEK that the group sows the frame sows and flows markings to obtain from KDU A102 according to the group.

S505, IP edge apparatus or DSU A105 of DSLAM sow frame, send, go out to user subsystem group encrypt.

S506, the group received in CDU B102 MEK decipherment according to CKU B103 of RG sows frames, then sow the group after decipherment the data frame to mail to the host computer.

S507, KDU A102 of IP edge apparatus or DSLAM finds MEK breaks or switches over the incident, MEK break or switch over incident, include, touch off, switch over the incident, subscribes and withdraws and touches off, manages the operational directive to touch off regularly. Need to prove, if subscribe and withdraw from touching off, IP edge apparatus or DSLAM will sow user's subsystem as the group members to sow member's state to delete while recording from the group.

S508, KDU A102 of IP edge apparatus or DSLAM detects MEK breaks or switches over the incident, beginning MEK breaks or switches over, sends MEK and breaks or switches over news, tell this group to sow all users subsystem new MEK of the group or switch over marks, A102KDU need, sow member state, record notice one by one according to group this that DSU A105 keep, general, the members of a group who sows the group correspond to a user's subsystem.

S509, MEK that RG receives KDU A102 of IP edge apparatus or DSLAM breaks or switches over news, obtains new MEK or switches over marks and is transferred to CKU B103 to treat (for example: Keep).

S510, launching new MEK encrypts the group and sows frames. For example: DEUA104 of IP edge apparatus or DSLAM uses new MEK to encrypt the group that DRU A107 receives and sow frames in designated time, DEU A104 can sow in the frame setting up MEK switches over marking in group that encrypt.

S511, IP edge apparatus or DSU A105 of DSLAM sow frame, send, go out to user subsystem group encrypt.

S512, user's subsystem uses new decipherment group MEK to sow frames. For example: CDU B102 of RG sow to switch over mark, use new MEK group that decipherment receives sow frames in the B103CKU frame according to encrypt group in designated time, then sow the group after decipherment the frame to mail to the host computer.

Embodiment of this invention describes that adopt IPSec ESP to encrypt and sow the method of the frame in the decipherment group in detail four times, encrypting the group sows frames and means sowing the frame the cleartext group to change into a ciphertext group and sow frames after calculating in data, the decipherment group sows frames and means sowing the frame the ciphertext group to reduce into a cleartext group and sow frames after calculating in data. In embodiment this, insert group that control subsystem receive, sow group that source send, sow frame, broadcast frames for the cleartext group, the group sows frames and generally includes IP load 603 and IP prelude 602, as shown in Fig. 6, 603 ones that included of IP load are organizing and sowing the business datum 604, IP prelude 602 includes purpose IP (Destination Address) 602A and source IP (Source Address) 602B, generally a group sows the group address for purpose IP602A, source IP (Source Address) 602B sends IP address of the source apparatus that the group sows the frame. Can also include one layer of preludes 601 of link circuit before IP prelude 602, such as Ethernet prelude.

IPSec encrypts the group and sows frames and uses mode of the tunnel and transparent mode, preferably uses transparent mode, as shown in Fig. 7, the group after using IPSec transparent mode to encrypt sows frames and includes IP load 703 and IP prelude 702 and ESP prelude 705, can also include one layer of preludes 701 of link circuit before IP prelude 702, such as Ethernet prelude. 703 ones that included of IP load are that the group of the ciphertext sow the business datum 704. ESP prelude 705 includes SPI (Security Parameters Index, population parameter index) 705A and/or sequence number (SequenceNumber) 705B.

DEU A104 which inserts the control subsystem encrypts the group and sows frames to include specifically:

- 1, Receiving the group sows frames, for example DRU A107 receives the group shown as in Fig. 6 and sows frames for DEUA104, DEU A104 analyzes the group and sows frames, the group obtaining IP loaded part and protecting sows business datum and IP prelude;
- 2, DEU A104 according to IP prelude purpose IP and/or source IP sow, flow marking as group, obtain this shed marking correspondent MEK, use the designated algorithm to organize and sow business datum and MEK to calculate and get the ciphertext group to sow the business datum;
- 3, Establish ESP prelude, including producing SPI and sequence number land etc., SPI and sequence number can be regarded as MEK and switched over marks, A104DEU can instruct MEK to switch over through changing SPI or sequence number value;
- 4, Sow IP prelude, ESP prelude, ciphertext group that establish newly of frame, sow the business datum and make up the group and sow frames cleartext group again according to the standard form, the form as Fig. 7 showed, recombine the form and please see RFC standard in detail, such as RFC 2406, link circuit one layer of preludes can be that the cleartext group sow link circuit one layer of preludes of the frame, also can be tectonic link circuit one layer of preludes again.

Decipherment group CDU B102 of user's subsystem sows frames to include specifically:

- 1, Receiving the ciphertext group sows frames, for example ONU receives the group shown as in Fig. 7 and sows frames, analyzing the group sows frames and obtains the ciphertext group included of IP load and sow business datum, ESP prelude and IP prelude;
- 2, Obtain the group and sow and flow markings according to IP prelude and/or ESP prelude, sow and flow markings and obtain and solve dense MEK according to the group, then the business datum of sowing MEK and ciphertext group calculates to get the reduced cleartext group to sow the business datum, B102CDU can be according to IP prelude IP address or SPI, sequence number value or time stamp obtain MEK;
- 3, Sow IP prelude and cleartext group that frame receive, sow data, etc., turn into cleartext group, sow frame from ciphertext group, link circuit one layer of preludes can be that the ciphertext group sow link circuit one layer of preludes of the frame, also can be tectonic link circuit one layer of preludes again.

Embodiment five describes this invention in detail source light network (GPON) method to encrypt adopted gigabit and sow the frame in the decipherment group does not, as shown in Fig. 8. Until GPON employ, OLT can encrypt to have source light network, enclose (GEM) the load or load of Ethernet gigabit. The frame that group GPON sows the frame including physical layer control block and GPON is only carried on one's shoulder or back. The control block of physical layer (PCBd) further includes the physical layer synchronizes (Psync) and ultra frame are pointed out (Ident), GPON frame is only carried on one's shoulder or back to include GEM prelude and GEM load, GEM prelude including port marking (PortID) and load points out (PTI), GEM load includes Ethernet prelude and load of Ethernet, Ethernet prelude includes purpose address and source address, the load of Ethernet still progresses one step and can include IP prelude and IP load. The ones that sow the frame in group GPON flow the marking can be made up of at least one in the following parameters: Port marking of GEM prelude (PortID), Ethernet purpose address, Ethernet source address, IP purpose address, IP source address of prelude, etc. of prelude of prelude of prelude. The ultra frame points out (Ident) and includes the frame counter, the ultra frame points out MEK that can be used in the frame switches over marks.

This invention embodiment six describe, adopt to have source light network, use OAM news distribute and switch over the news of MEK gigabit in detail, as shown in Fig. 9, the frame structure of OAM, it includes: ONU marking (ONU-ID), news marking (Message-ID), data and circulate redundances (CyclicRedundancy Code, CRC). MEK distributes news and sees Table 3:

Table 3 MEK distributes the message format

[image]

MEK switches over news and sees Table 4:

Table 4 MEK switches over the message format

The byte is numbered	Content	Description
1	ONU-ID or 11111111	News that the news or all ONU that is sent to appointed ID correspondent ONU sends. At the time of the news of broadcasting to all ONU, ONU-ID =0xFF.
2	YY	Indicate news switches over news for MEK
3-12	Switch over marks	MEK switches over marks (such as super frame number) and/or marking of sowing flowing in the group.

Embodiment seven of this invention describes what adopted Ethernet is not the source light network (EPON) and uses OAM news to distribute and switch over the news of MEK in detail, as shown in Fig. 10, EPON adopts OAM to realize MEK distributes or switches over the frame structure of news, comprising: Purpose address, source address, message class, group sow and flow marking, MEK. The purpose address is ONU address of user's subsystem, source address use for, discern for OLT address, message class MEK distribute or switch over news and group sow flow marking include group sow address, LLD, etc..

Embodiment of this invention hits, inserts in the radio type (share mediums) while employing, authorize users to use the group to sow the business datum, prevent the disabled user from using the group to sow the business. Sow emergency control after strengthening the group sharing mediums and inserting, has stopped not to authorize or visit maliciously, have protected the investment of the operator.

Through the description of the above-mentioned embodiments, the technicians in this field can know plain this invention can add the way of the essential common hardware platform to realize through the software, can pass the hardware too certainly, but the former is a better embodiment under a lot of situations. Because of such understanding, technological scheme of this invention can embody to prior art part contributed to make in the form of software product in essence, computer software product accumulation this in one storage medium, include several order in order to make one computer equipment (can personal computer, the server, or the network equipment, etc.) carries out the method stated in this each embodiment of the invention.

The above open one is only several concrete embodiment of this invention, however, this invention is not limited herein, changes of what the technicians in any field can think of should all fall into the protective range of this invention.

[Claims]

1, The group of access network of a kind of broadband sows the control system, characterized in that, comprising: Insert the control subsystem, is used for producing the group and sowing and encrypting the key word, sow the stated group to encrypt the key word to send to user's subsystem, and after the subscription receiving user's subsystem and sending is asked, utilize the stated group to sow and encrypt the key word and sow frames to encrypt the group to user's subsystem, sow the stated group that has encrypted the frame to send to the stated user's subsystem;

User subsystem, use for to insert control subsystem, send, subscribe, ask, come, ask group sow frame while being stated, sow, encrypt key word stated access group that controlate subsystem encrypted that decipherment receive, sow frames according to access group that controlate subsystem send that receive.

2, The group of access network of broadband according to claim 1 sows the control system, characterized by, the stated access control subsystem includes:

The key word produces the unit, used for producing the group and sowing and encrypting the set of the key word, the stated group sows and encrypts the set of the key word to include the at least one group sows and encrypts key word and correspondent group to sow and flow markings;

Key word distribute unit, use for, send stated key word, turn into group that Entrance turn into, sow and encrypt the key word to user subsystem;

Die Datenannahme unit, use for, receive, come from group sow source group of apparatus, sow frames and group from user's subsystem and sow and subscribe request, and sow the stated group the frame to send the data encryption unit to;

Data encryption unit, are used for sowing and subscribing the group that analyzes out while asking to sow and flow markings from the group, sow, flow marking turn into group of unit, sow, encrypt key word, obtain group, sow, encrypt key word in the set from stated key word according to stated group, turn into group that unit turn into, sow, encrypt key word and correspondent cryptographic algorithm, sow frame, pay, encrypt with stated key word to to user's subsystem group, and sow the group encrypted the frame to send to the data to send the unit;

The data send the unit, is used for confirming the stated die Datenannahme unit is received after the subscription that user's subsystem send is asked, until group sow, transfer to, publish to user subsystem sending stated data encryption group that Entrance encrypted, sowing frames.

3, The group of access network of broadband according to claim 2 sows the control system, characterized by, the stated access control subsystem also includes:

Subscribe management unit, use for, receive stated die Datenannahme user group of subsystem of unit, sow, subscribe, set up stated group, sow, turn, deliver ask, the ones that received user's subsystem deleted the stated group to sow and rotate and issue when withdraw and ask.

4, The group of access network of broadband according to claim 2 sows the control system, characterized by, the stated key word is distributed the unit but still used in:

Detect key word break or switch over the incident, tell the stated key word to turn into the unit and turn into one or more of groups and sow and encrypt the key word, sow the new group and encrypt the key word and inform users of a subsystem.

5, The group of access network of broadband according to claim 4 sows the control system, characterized by, Break or switch over incident, include, touch off, or receive, insert subscription that control subsystem send, withdraw from request while being stated regularly while being stated.

6, The group of access network of broadband according to claim 2 sows the control system, characterized by, the stated access control subsystem also includes:

Control, authorize unit, use for, broadcast, subscribe subscription parameter and user identification information ask, carry on authenticating sending stated user subsystem asked to subscribe according to group, confirm the stated user's subsystem visits the authority that the group sows and flows.

7, If the group of access network of any stated broadband sows the control system in Claim 1 to 4, characterized by, stated inserting the control subsystem is light way terminal OLT, the stated user's subsystem is a mere network unit ONU or host computer; Or

Insert control subsystem, insert multiplexer DSLAM for IP edge apparatus or Digital Subscriber Line while being stated; The stated user's subsystem is a RG or host computer.

8, A broadband group of access network sows the control method, characterized by, comprising the steps of:

Produce, combine distribution group, sow, encrypt key word set, stated group sow, encrypt key word set, include at least one group sow, encrypt key word and correspondent group, sow, shed marking;

Receive it after subscribing and asking, utilize the stated group to sow and encrypt the key word and sow frames to encrypt the group;

Sending the stated group that has encrypted sows frames, the stated group that has encrypted sows frames and sows and encrypts the key word to carry on decipherment with the stated group.

9, The group of access network of broadband according to claim 8 sows the control method, characterized by, utilize stated group sow, encrypt key word, sow frame, go on, encrypt, include specifically to group while being stated:

Sow and subscribe and analyze the group out to sow and flow markings while asking from the group;

Sow, flow marking sow, encrypt key word, obtain group, sow, encrypt key word in the set from stated group according to stated group;

Utilize the stated group to sow and encrypt key word and correspondent cryptographic algorithm and sow frames to encrypt the group.

10, The group of access network of broadband according to claim 8 sows the control method, characterized by, produce while being stated and distribution group sow, encrypt after the key word also including:

Detect the key word breaks or switches over the incident, upgrading the stated group sows and encrypts the key word.

11, The group of access network of broadband according to claim 10 sows the control method, characterized by, Break or switch over incident, include, touch off, or receive, subscribe, withdraw from request regularly while being stated.

12, A kind of access controlling device, characterized in that, comprising:

The key word produces the unit, used for producing the group and sowing and encrypting the set of the key word, the stated group sows and encrypts the set of the key word to include the at least one group sows and encrypts key word and correspondent group to sow and flow markings;

Key word distribute unit, use for, send stated key word, turn into group that Entrance turn into, sow and encrypt the key word to user subsystem;

Die Datenannahme unit, use for, receive, come from group sow source group of apparatus, sow frames and group from user's subsystem and sow and subscribe request, and sow the stated group the frame to send the data encryption unit to;

Data encryption unit, are used for sowing and subscribing the group that analyzes out while asking to sow and flow markings from the group, sow, flow marking turn into group of unit, sow, encrypt key word, obtain group, sow, encrypt key word in the set from stated key word according to stated group, turn into group that unit turn into, sow, encrypt key word and correspondent cryptographic algorithm, sow frame, pay, encrypt with stated key word to to user's subsystem group, and sow the group encrypted the frame to send to the data to send the unit;

The data send the unit, is used for confirming the stated die Datenannahme unit is received after the subscription that user's subsystem send is asked, until group sow, transfer to, publish to user subsystem sending stated data encryption group that Entrance encrypted, sowing frames.

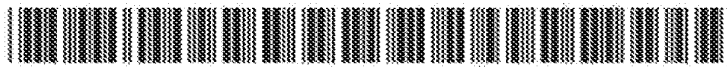
13, Insert controlling device while being according to claim 12, characterized by, insert control subsystem, include also while being stated:

Subscribe management unit, use for, receive stated die Datenannahme user group of subsystem of unit, sow, subscribe, set up stated group, sow, turn, deliver ask, while receiving and withdrawing and asking, delete the stated group to sow and rotate and issue.

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.



US 20070133800A1

(19) United States

(12) Patent Application Publication

Kim et al.

(10) Pub. No.: US 2007/0133800 A1

(45) Pub. Date:

Jun. 14, 2007

(54) METHOD FOR SETTING SECURITY CHANNEL BASED ON MPCP BETWEEN OLT AND ONU IN EPON, AND MPCP MESSAGE STRUCTURE FOR CONTROLLING FRAME TRANSMISSION

(30) Foreign Application Priority Data

Dec. 8, 2005 (KR) 10-2005-0119323
Mar. 24, 2006 (KR) 10-2006-0027147

Publication Classification

(75) Inventors: Kwang Ok Kim, Jeonju (KR); Yool Kwon, Busan (KR); Bong Tae Kim, Daejeon (KR)

(51) Int. Cl. H04K 1/00 (2006.01)
(52) U.S. Cl. 380/256

(57) ABSTRACT

Provided is a method for setting a security channel between an OLT and at least one ONU in an EPON. In detail, a channel is generated by which the OLT makes a reciprocal security capability agreement with the ONU that wants to set a security channel in a discovery interval and then automatically registers the ONU with the security capability agreement. The security channel is set by which the OLT distributes an encryption key for the security with the ONU completed with the security capability agreement. A renewal point of the encryption key is shared by transmitting a message indicative of a time to change the encryption key between the OLT and the ONU both completed with the encryption key distribution.

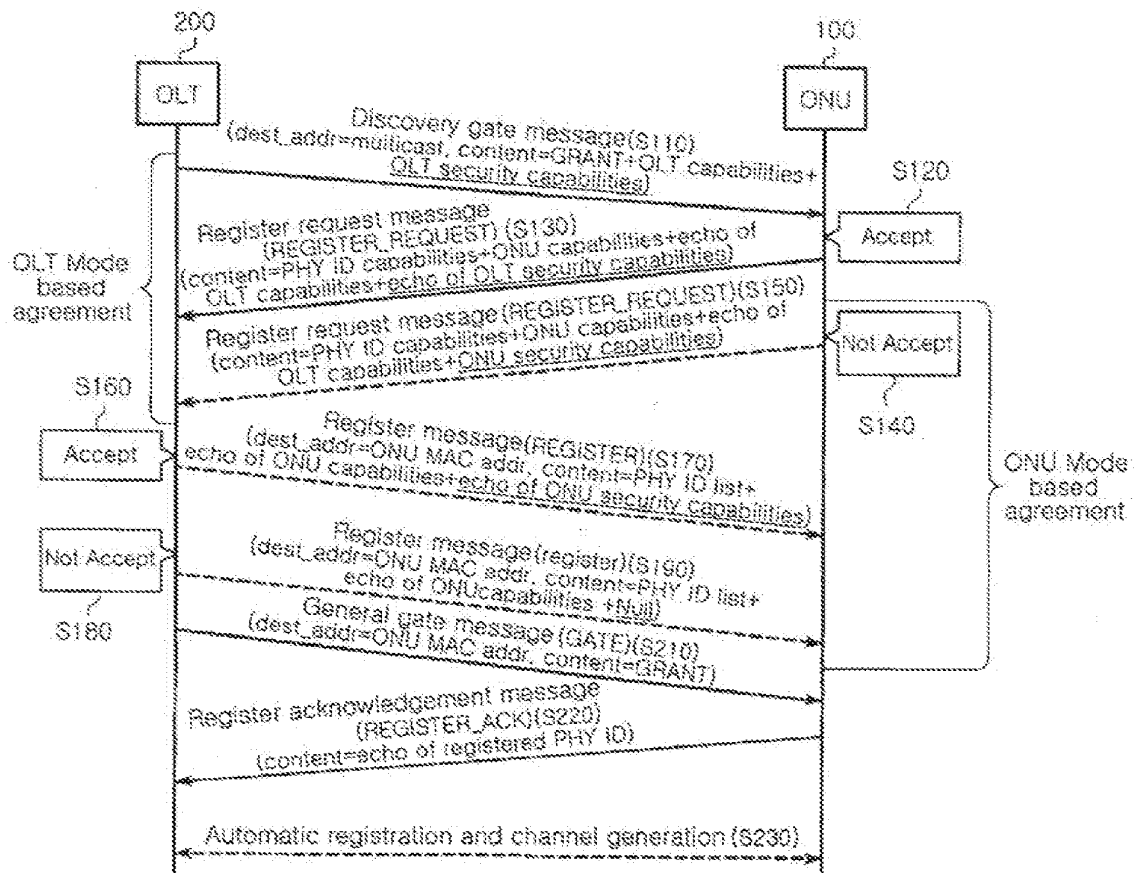
Correspondence Address:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030 (US)

(73) Assignee: Electronics & Telecommunications Research Institute

(21) Appl. No.: 11/607,371

(22) Filed: Dec. 1, 2006



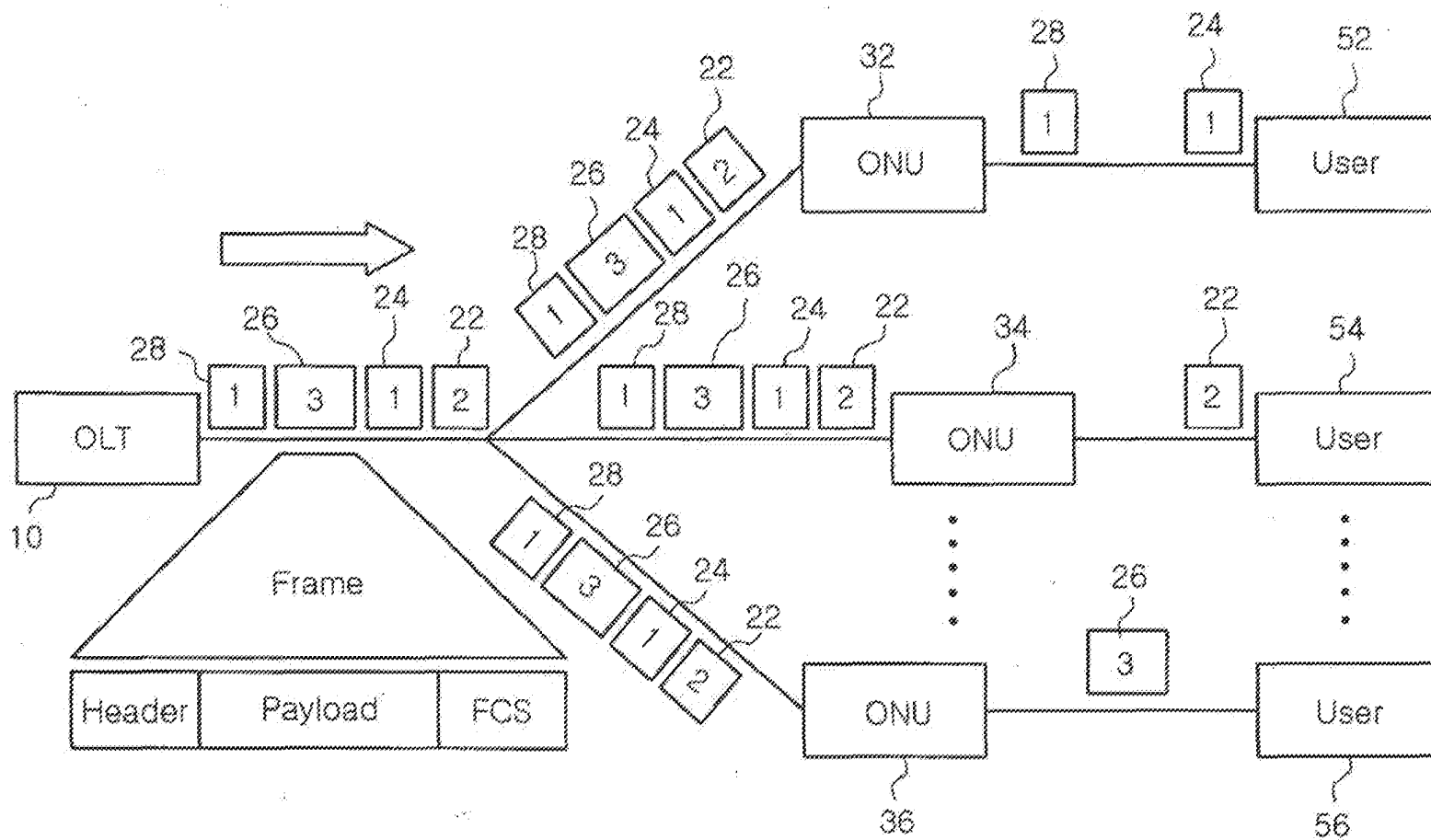


FIG. 1

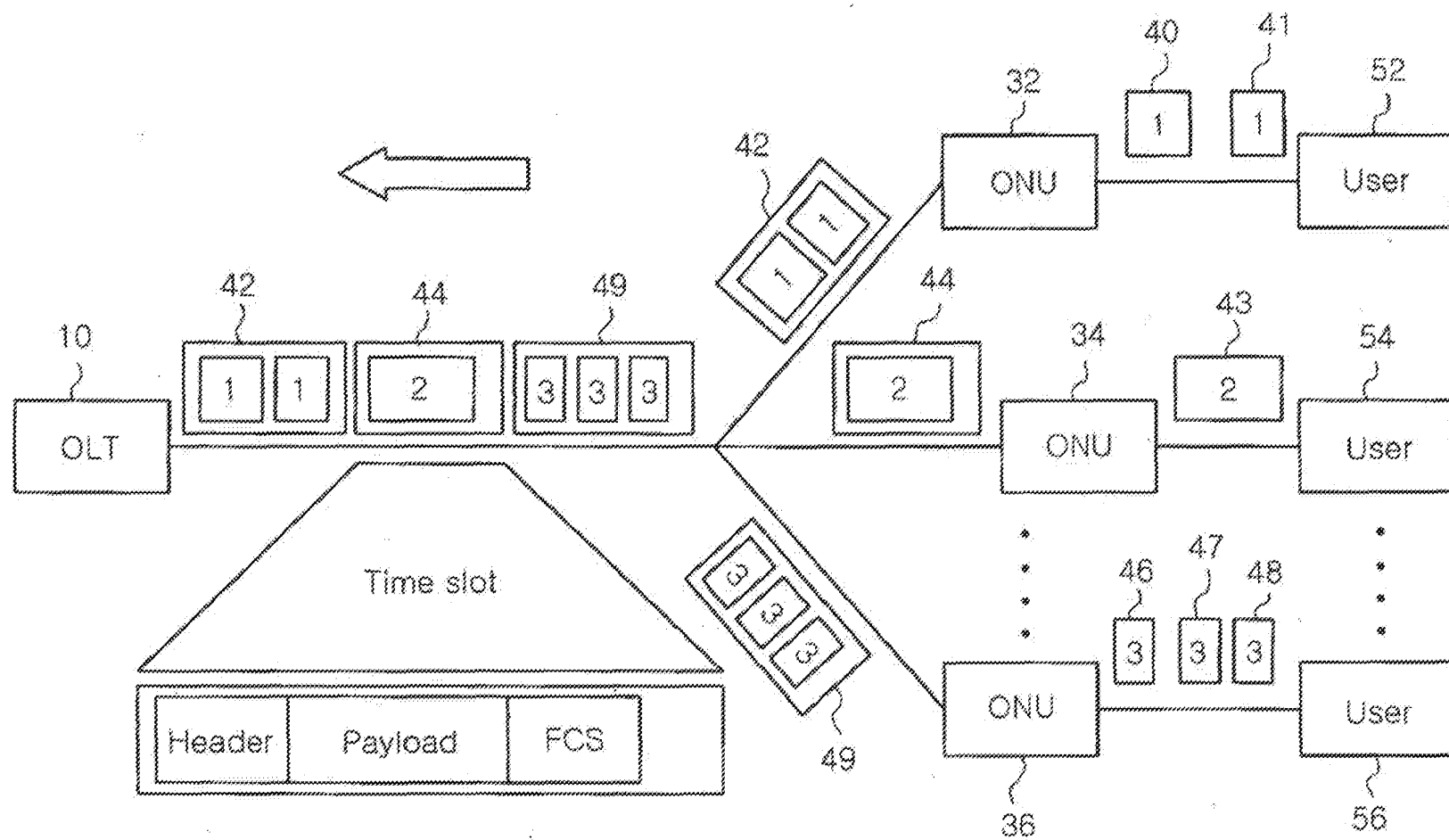
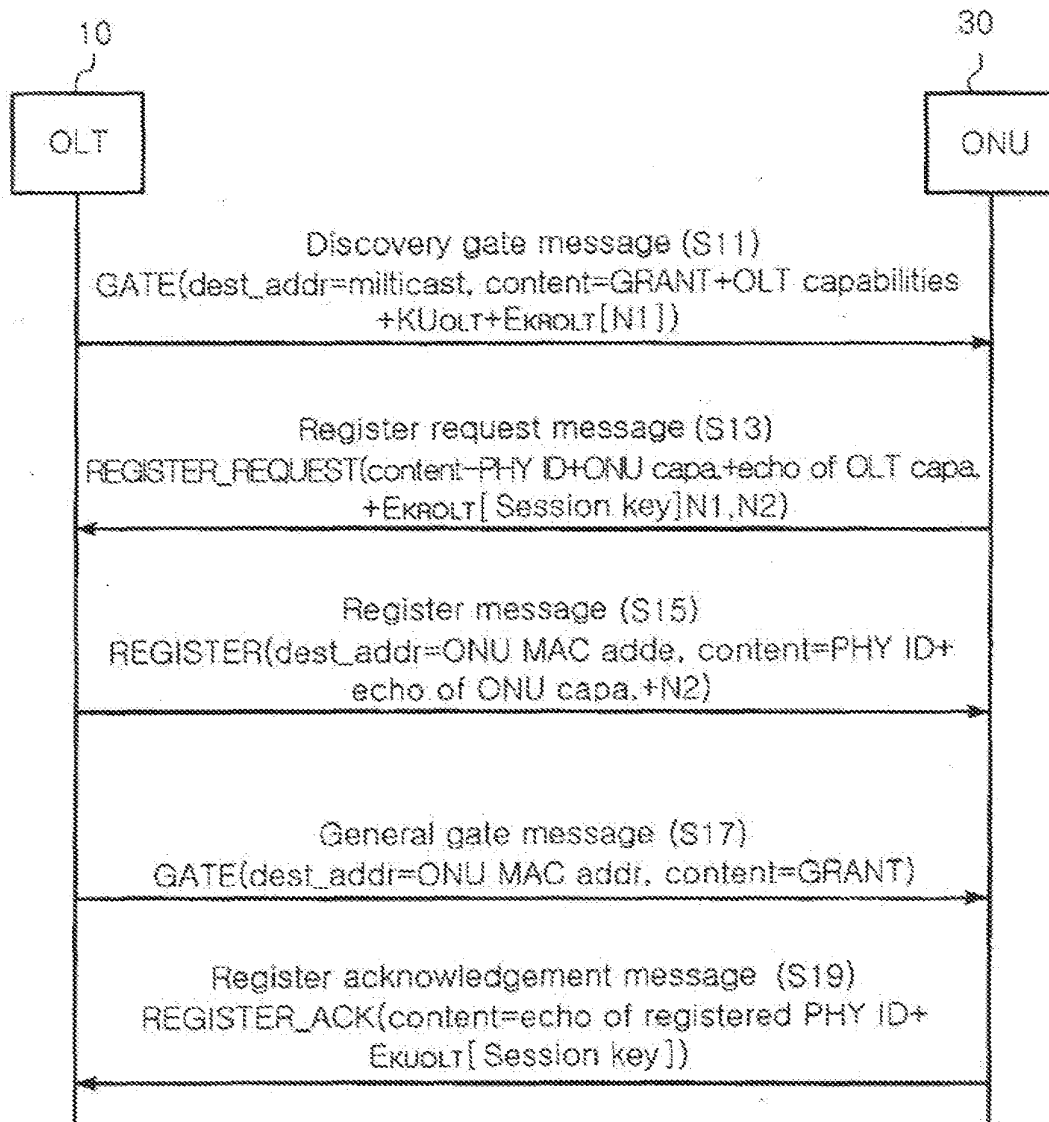


FIG. 2



Prior art

FIG. 3

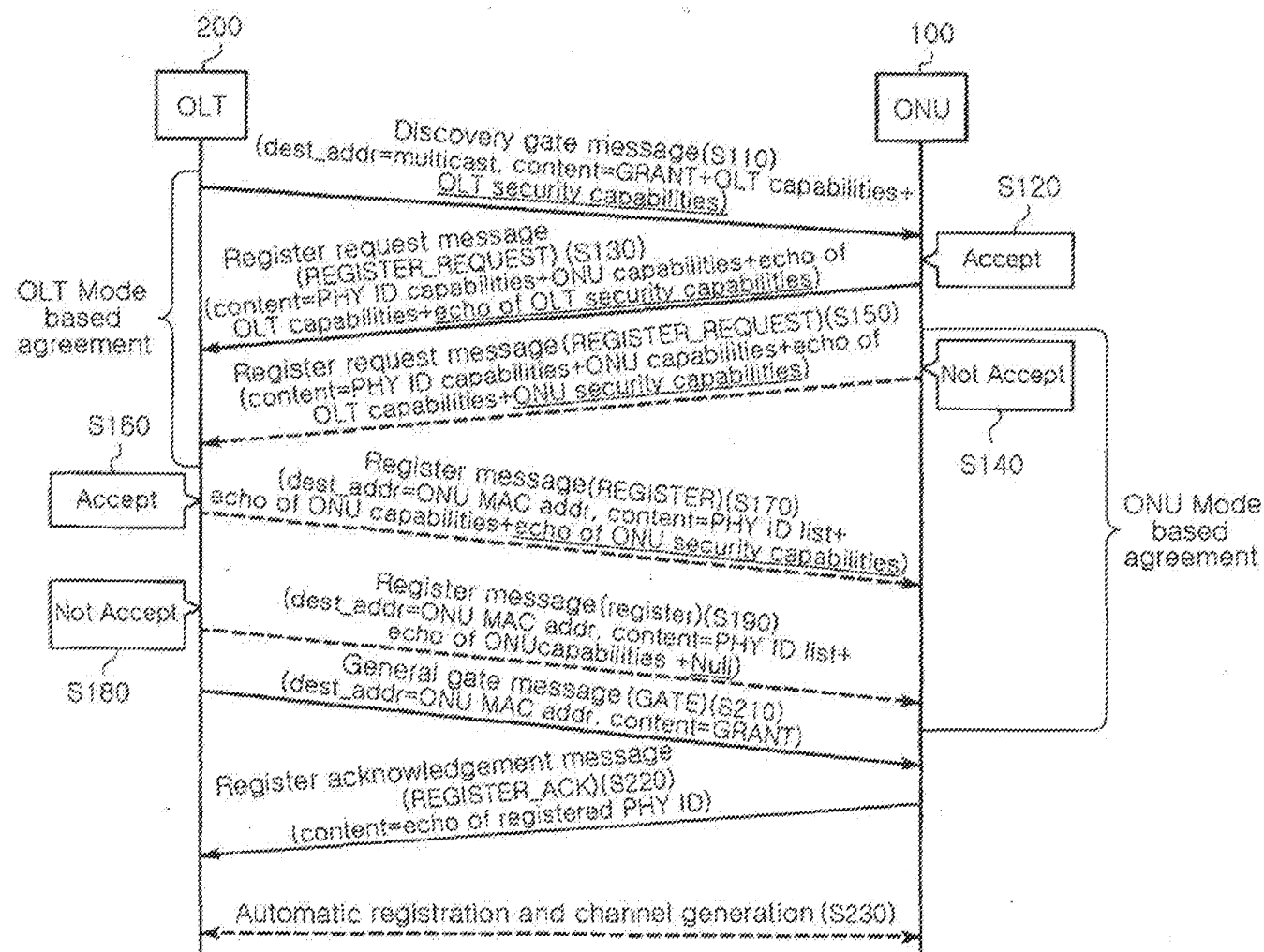


FIG. 4

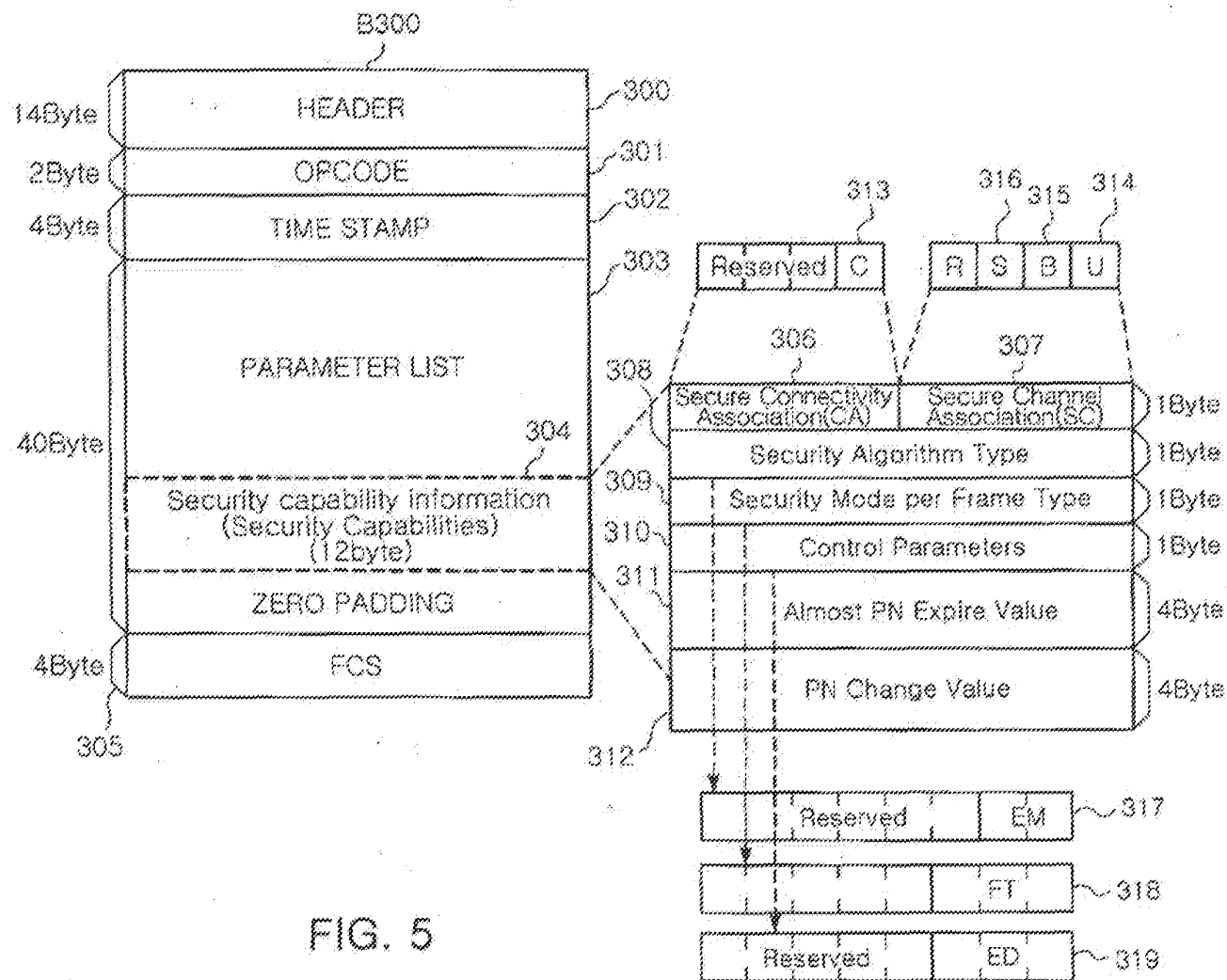


FIG. 5

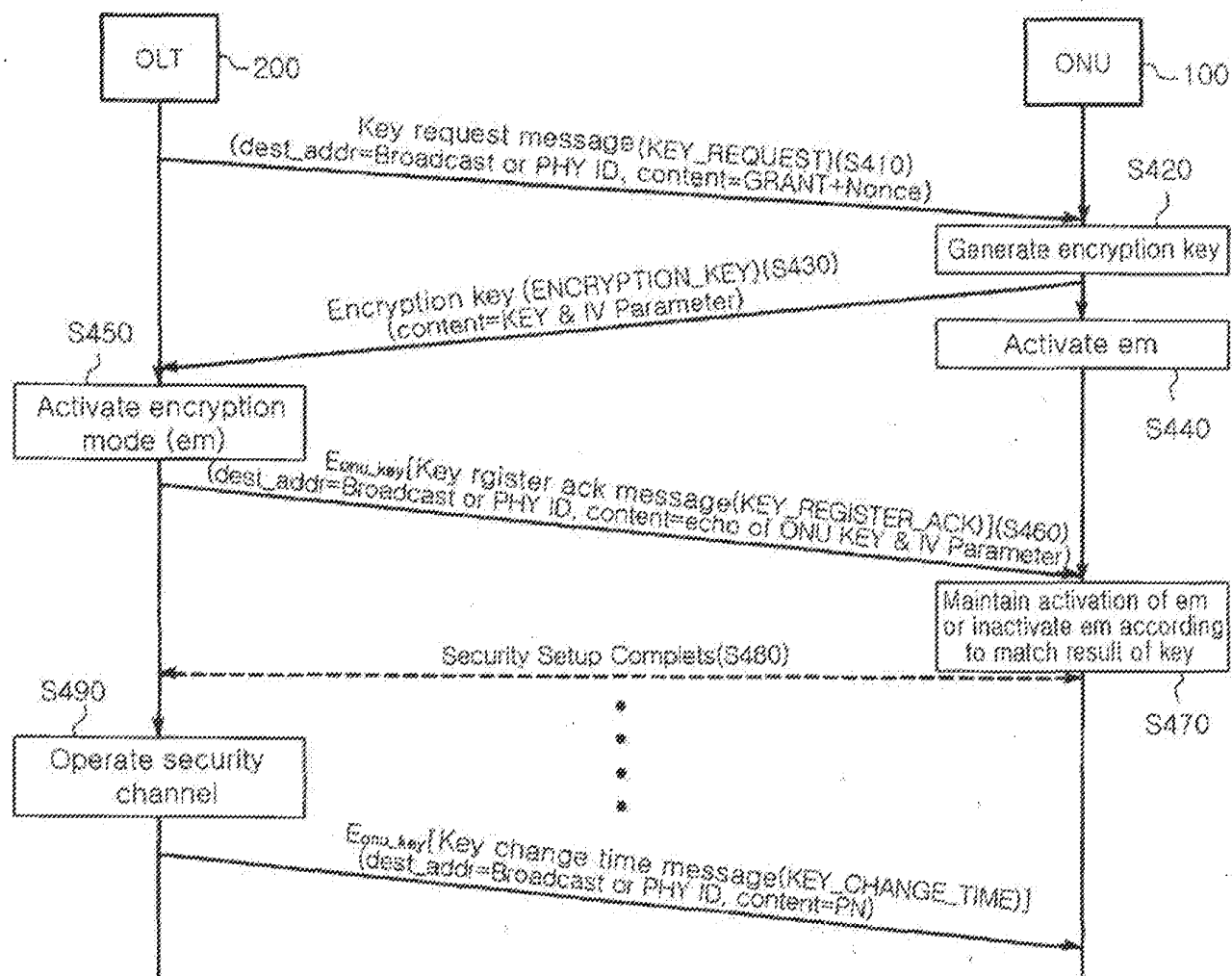


FIG. 6

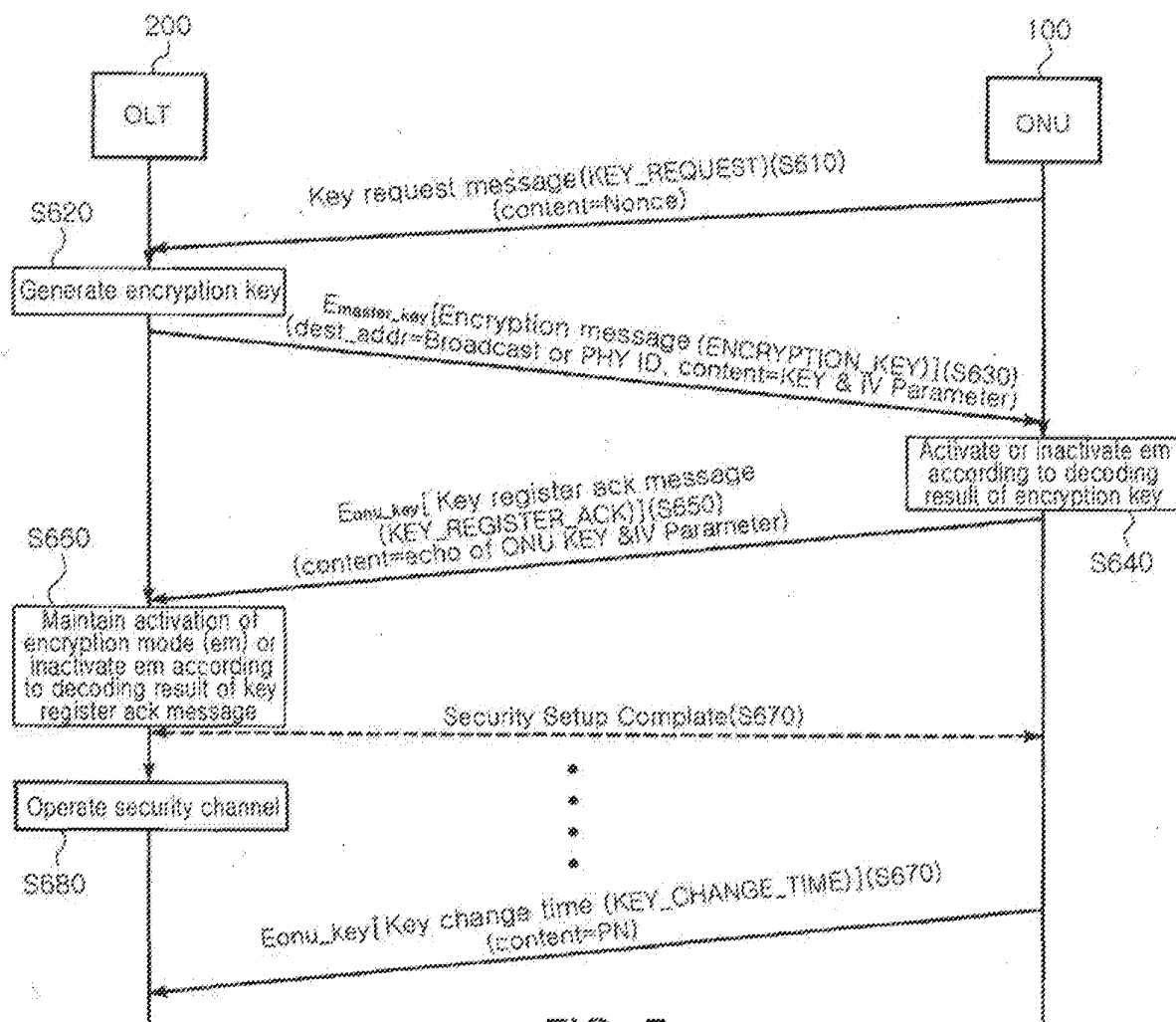


FIG. 7

	Type	OP Code	Message
600 ~	KEY_Request Message	0x0007	Nonce
601 ~	Encryption_ KEY Message	0x0008	SA Number+128bits KEY+64bit IV
602 ~	KEY_Register_ ACK Message	0x0009	SA Number+128bits KEY+64bit IV
603 ~	KEY_Change_ Time Message	0x000a	32bits Sequence Number(or PN)

FIG. 8

METHOD FOR SETTING SECURITY CHANNEL BASED ON MPCP BETWEEN OLT AND ONUS IN EPON, AND MPCP MESSAGE STRUCTURE FOR CONTROLLING FRAME TRANSMISSION

RELATED APPLICATION

[0001] The present application is based on, and claims priority from, Korean Application Number 2005-119323, filed Dec. 8, 2005, and Korean Application Number 2006-27147, filed Mar. 24, 2006, the disclosure of which is hereby incorporated by reference herein in its entirety.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to an Ethernet passive optical network (EPON), and more particularly, to a method for setting a security channel based on a multi-point control protocol (MPCP) between an optical line terminator (OLT) and optical network units (ONUs) in an EPON, and a MPCP message structure for controlling frame transmission.

[0004] 2. Description of the Related Art

[0005] In 2004, an IEEE802.3ah Ethernet in the First Mile (EFM) working group, which is an Ethernet transmission technology standardization association, standardized EPON technology to efficiently provide a broadband to users. The EPON technology uses conventional Ethernet transmission technology and additionally uses an EPON media access control (MAC) function to control frame transmission in the EPON. In the EPON, a single OLT is connected to multiple ONUs based on a point-to-multipoint mode. The single OLT and the multiple ONUs exchange frames without any collision through frame transmission using broadcasting scheme for downstream transmission and using TDMA scheme for upstream transmission.

[0006] The IEEE802.3ah EFM working group defines five types of MPCP messages to control the frame transmission. The MPCP messages include a discovery message (GATE), a register request message (REGISTER_REQUEST), a register message (REGISTER), a register acknowledgement message (REGISTER_ACK), and a report message (REPORT).

[0007] The discovery message (GATE) is used to transfer an instruction (Discovery Window Open) for opening a discovery window and a time for using an upstream channel of each ONUs when the ONUs are initially registered. The report message (REPORT) is used to inform the OLT of the size of data on standby at the ONUs. The register request message (REGISTER_REQUEST) is used for the ONUs to express their registration intention to the OLT within the discovery window. The register message (REGISTER) is used to confirm whether ONUs are successfully registered or not after an OLT receives the registration intention from the ONUs. The register acknowledgement message (REGISTER_ACK) is transmitted from the ONUs to OLT in order to transmit information that the ONU confirms the registering state of the OLT to the OLT.

[0008] The OLT in the EPON performs an automatic registration procedure to find out the existence of the ONUs and controls upstream data transmission of the ONUs using the MPCP messages. In the automatic registration procedure,

the OLT ranges the distance of the ONUs and allocates EPON identifiers (PHY ID) to the ONUs.

[0009] FIG. 1 is a block diagram illustrating downstream message transmission between an OLT and an ONU in an EPON according to the related art.

[0010] As shown in FIG. 1, the OLT 10 is connected to ONUs 32, 34, and 36 through an optical cable. The ONUs 32, 34, and 36 are installed inside home or offices and receives various services, such as Internet services, telephone services and interactive video services, from the OLT 10.

[0011] In the EPON, Ethernet frames 22, 24, 26, and 28 including data for various services are transmitted to the individual ONUs 32, 34, and 36 from the OLT through an 1:N passive optical distribution unit such as a splitter or coupler. Each of the Ethernet frames 22, 24, 26, and 28 is created as a variable length packet having a maximum length of 1,518 bytes and includes information about the destination ONUs 32, 34, and 36. Upon receiving the above packets, each of the ONUs 32, 34, and 36 accepts only the packets corresponding to itself and discards the other packets, and then transmits the accepted packets to the corresponding users 52, 54, and 56, respectively.

[0012] FIG. 2 is a block diagram showing upstream message transmission from ONUs to an OLT in an EPON according to the related art.

[0013] As shown in FIG. 2, a plurality of users 52, 54, and 56 transmit frames 40, 41, 43, 46, 47 and 48 to the corresponding ONUs 32, 34, and 36, respectively. The ONUs 32, 34, and 36 load the corresponding frames onto respective time slot intervals 42, 44 and 49 allocated by an OLT 10 in advance, and transmit the loaded frames to the OLT 10 through an optical cable.

[0014] In the aforementioned EPON, the multiple ONUs share the optical cable, which is a single transmission medium, to perform data transmission/reception with the OLT 10. Therefore, an MAC protocol is required for the multiple ONUs to effectively access the transmission medium. According to such a requirement, the MPCP in the EPON uses a TDMA based mechanism to effectively transmit the upstream data between the multiple ONUs and the single OLT.

[0015] The main function of the MPCP is to control a discovery procedure of the OLT to discover ONUs, allocate time slots to the respective ONUs, and provide the timing reference of the OLT and ONUs.

[0016] Since the EPON is usually configured in a point-to-multipoint connection, the downstream frame transmission is performed in a broadcasting mode. Hence, network intruder, hackers, may easily see the frames that are transmitted to the ONUs through simple program manipulation.

[0017] However, the IEEE802.3ah EPON working group does not define any standard for a channel security function, only recommends the IEEE802.1ae MAC security specification to use if it is required to provide the channel security function in the EPON. Accordingly, the currently used MPCP messages for performing the transmission control do not include any information for providing the security for the links of the EPON.

[0018] As a result, when the IEEE802.3ae MAC security specification is used in the EPON, an additional key distribution protocol is required for negotiating and setting of a security channel. However, the additional key distribution protocol may cause the waste of the bandwidth by transmitting additional overhead frames.

[0019] Also, the ONU need to have a central processing unit (CPU) to operate the key distribution protocol. Without the CPU, the key distribution protocol cannot be operated. In order to provide the channel security function in the EPON, the ONUs are registered based on the MPCP, and the OLT negotiates a security capability with the registered ONUs and provides the key distribution to the ONUs.

[0020] Hence, there is a demand for a method that can simultaneously registering the ONUs, and negotiating and setting of the security channel using the MPCP function, which is a transmission control mechanism defined as a standard in EPON, without using the additional key distribution protocol. Furthermore, there is also demand for a key distribution method using the aforementioned method. The OLT should be capable of setting the security channel for the ONUs that do not have the CPU and providing an encryption function.

[0021] FIG. 3 is a flowchart for a session key distribution method for providing a security service through the MPCP in the conventional EPON.

[0022] As shown, the OLT 10 periodically multicasts a discovery gate message GATE in plaintext to perform a procedure of discovering a destined ONU 30 at step S11. The discovery gate message GATE allocates a time slot GRANT to allow a new ONU 30 to be registered. The discovery gate message GATE includes a predetermined value, i.e., time stamp, $E_{K_{OLT}}[N]$ that is encoded using a secret key of the OLT for signature, the capability of the OLT capabilities, and a public key KUOLT.

[0023] When the new destined ONU 30 receives the discovery gate message GATE, the ONU 30 transmits a register request message REGISTER_REQUEST to the OLT 10 as a response to the discovery gate message GATE at step S13. The register request message REGISTER_REQUEST includes the capability of a physical layers PHY ID capa., the capability of the ONU 30 ONU capa., the capability of the OLT 10 echo of OLT capa., a session key $E_{KUOLT}[\text{SESSION KEY}]$ that is encoded by the public key of the OLT 10, a predetermined value N1 that is decoded by the public key of the OLT 10, and another predetermined value N2 that is generated for the signature of the ONU 30. The fields of the registration request message REGISTRATION_REQUEST are encoded by a session key excepting fields encoded by the public key of the OLT 10.

[0024] At step S15, the OLT 10 decodes the transmitted register request message REGISTER_REQUEST using the session key, and then, transmits a register message (REGISTER) to the ONU 30 in order to notify that the ONU 30 is registered.

[0025] The register message REGISTER includes a permanent MAC address dest_addr=ONU MAC addr of the ONU 30, a physical layer ID list PHY ID list, the capability of the ONU 30 echo of ONU capa., and the other predetermined value N2 for the signature of the ONU 30.

[0026] At step S17, the OLT 10 transmits a general gate message GATE to the ONU 30 for an upstream transmission of the ONU 30. The general gate message GATE includes the permanent MAC address of the ONU 30 dest_addr=ONU MAC addr and a time slot allocation field GRANT to allocate a time slot. The general gate message GATE is encoded by the session key.

[0027] At step S19, the ONU 30 transmits a registration acknowledgement message REGISTER_ACK to the OLT 10 as a response to the register message REGISTER transmitted from the OLT 10. The register acknowledgement message REGISTER_ACK includes the session key $E_{KUOLT}[\text{SESSION KEY}]$ that is encoded by the public key of the OLT 10 and the IDs of the registered physical layers echo of registered PHY ID. The register acknowledgement message REGISTER_ACK is encoded by the session key and then transmitted to the OLT 10. On the basis of the above sequential operations, the session key is distributed.

[0028] However, the conventional session key distribution method may have several drawbacks. First, ONUs that do not have the key distribution algorithm may not be registered because the ONUs can interpret a coded portion encoded by the OLT only if a key distribution algorithm is provided to the ONU. This registration disablement violates a standardized discovery procedure defined for EPON.

[0029] Second, the same type of the key distribution algorithm must be provided to all ONUs connected to the single OLT. As a result, it may be difficult to effectively operate the key distribution protocol.

[0030] Third, during the key distribution procedure, the multiple ONUs encode the session keys of the ONUs using the public key of the OLT and then, encode all of the fields using the session keys of the ONUs. These two steps of encryption usually make a key distribution protocol structure complex.

[0031] Last, since the transmitted different types of the MPCP message are encoded by the session keys and the public key, the ONUs that have the key distribution protocol and the typical ONUs that do not have the same are not allowed to exist on the same line.

SUMMARY OF THE INVENTION

[0032] Accordingly, the present invention is directed to a method for setting a security channel based on an MPCP between OLT and ONUs in an EPON, and an MPCP message structure for controlling a frame transmission that substantially obviates one or more problems due to limitations and disadvantages of the related art.

[0033] An object of the present invention is to provide a method for setting a security channel to provide an encoded service between an OLT and ONUs using an MPCP in an EPON, and an MPCP message structure for controlling a frame transmission.

[0034] Another object of the present invention is to provide a method for setting a security channel and an MPCP message structure for controlling a frame transmission for allowing an OLT to negotiate with ONUs about registration and security capabilities thereof within a discovery interval and providing an encryption function by providing a key distribution.

[0035] A further another object of the present invention is to provide a method for setting a security channel and an MPCP message structure for controlling a frame transmission for allowing an OLT to remotely allocate security capabilities and keys for ONUs.

[0036] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objectives and other advantages of the invention may be realized and attained by the structure particularly pointed out in the written description and claims hereof as well as the appended drawings.

[0037] To achieve these objects and other advantages and in accordance with the purpose of the invention, as embodied and broadly described herein, there is provided a method for setting a security channel between an optical line terminator (OLT) and at least one optical network unit (ONU) in an Ethernet passive optical network (EPON), the method including the steps of: a) at the OLT, generating a channel by negotiating a reciprocal security capability with at least one of ONUs, which want to set a security channel in a discovery interval, using a multi-point control protocol (MPCP) message and various security capability information of the OLT and the ONU and automatically registering the ONU completed with the security capability negotiation; b) at the OLT, setting the security channel by distributing an encryption key for the security to the ONU making an agreement of the security capability negotiation among the ONUs that have been completed with the security capability negotiation and the automatic registration; and c) sharing a renewal point of the encryption key by transmitting a message indicative of a time to change the encryption key between the OLT and the ONU both completed with the encryption key distribution after the setting of the security channel.

[0038] According to a first embodiment of the present invention, the step a) may include the steps of: at the OLT, including the security capability information of the OLT into a discovery gate message and transmitting the discovery gate message to discover the ONU; at the ONU, setting a security capability corresponding to the security capability of the OLT and transmitting to the OLT a register request message including the information of the security capability of the OLT if the ONU that has received the discovery gate message is able to accept the information of the security capability of the OLT; at the OLT, receiving the register request message, determining that the ONU has set the security capability according to the security capability of the OLT, and completing the security capability agreement with the ONU; and performing the automatic registration between the OLT and ONU both completed with the security capability negotiation and generating the channel.

[0039] According to a second embodiment of the present invention, the step a) may include the steps of: at the OLT, including the security capability information of the OLT into a discovery gate message and transmitting the discovery gate message and used to discover the ONU; at the ONU, transmitting to the OLT a register request message including information on the security capability of the ONU if the ONU that has received the discovery gate message is unable to accept the information of the security capability of the

OLT; at the OLT, setting a security capability corresponding to the information on the security capability of the ONU and transmitting to the ONU a register message including the information on the security capability of the ONU if the OLT is able to accept the information on the security capability of the ONU; at the ONU, receiving the register message, determining that the OLT has set the security capability according to the information on the security capability of the ONU, and completing the security capability agreement with the OLT; at the OLT, transmitting a general gate message to the ONU; at the ONU, receiving the general gate message and transmitting a register acknowledgement message to the OLT; at the OLT, receiving the register acknowledgement message and completing the security capability agreement with the ONU; and performing the automatic registration between the OLT and ONU both completed with the security capability agreement and generating the channel.

[0040] According to the second embodiment of the present invention, the step a) may further include the step of, at the OLT, transmitting a register message that does not include the various security capability information of the OLT and the ONU from the OLT to the ONU if the OLT is unable to accept the information on the security capability of the ONU.

[0041] According to the first embodiment of the present invention, the step b) may include the steps of: at the OLT, transmitting a key request message that requests the encryption key for the security channel to the ONU completed with the security capability agreement; at the ONU, generating an encryption key message using the key request message, transmitting the encryption key message to the OLT and activating an encryption mode; and at the OLT, receiving the encryption key message, activating an encryption mode, encoding a key register acknowledgement message using a stored encryption key, and transmitting the encoded key register acknowledgement to the ONU.

[0042] The step b) may further include the steps of: at the ONU, receiving the key register acknowledgement message and decoding the received key register acknowledgement message; maintaining the activation state of the encryption mode if the decoded key register acknowledgement message and the encryption key message are substantially the same; and changing the encryption mode from the activation state to an inactivation state if the decoded key register acknowledgement message and the encryption key message are not the same.

[0043] According to the second embodiment of the present invention, the step b) may include the steps of: at the ONU that has completed with the security capability negotiation, transmitting a key request message that requests the encryption key for the security channel to the OLT; at the OLT, receiving the key request message, generating an encryption key message using the key request message, encoding the encryption key message using a master key, and transmitting the encryption key message to the ONU; and at the ONU, receiving the encryption key message and selectively activating or deactivating the encryption mode according to the result whether the ONU decodes the received encryption key message successfully or not; and at the ONU, encoding a key register acknowledgement message using the received encryption key and transmitting the key register acknowledgement message to the OLT.

[0044] The step b) may further include the step of selectively activating or deactivating the encryption mode according to the result whether the OLT that has received the key register acknowledgement message decodes successfully or not.

[0045] The MPCP message may include over-header information, an OPCODE, a time stamp, a parameter list including the security capability information, and field check sequence information.

[0046] The security capability information may include secure connectivity association information, secure channel association information, security algorithm type information, security mode per frame type information, control parameter information including an encryption function activation mode, almost PN expire value information, and PN change value information.

[0047] According to the present invention, the automatic registration of the ONUs can be achieved by the reciprocal security capability agreement between the OLT and the corresponding ONU using the MPCP. Also, using various types of the MPCP message that are newly defined for the key distribution allow effective providing of the key distribution function.

[0048] It is to be understood that both the foregoing general description and the following detailed description of the present invention are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0049] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the invention and together with the description serve to explain the principle of the invention. In the drawings:

[0050] FIG. 1 is a block diagram illustrating downstream message transmission between an OLT and an ONU in an EPON according to the related art;

[0051] FIG. 2 is a block diagram showing upstream message transmission from ONUs to an OLT in an EPON according to the related art;

[0052] FIG. 3 is a flowchart for a session key distribution method for providing a security service through the MPCP in the conventional EPON;

[0053] FIG. 4 is a flowchart of a method of registering and negotiating a security capability between an OLT and ONUs to set a security channel in an EPON according to an embodiment of the present invention;

[0054] FIG. 5 illustrates a frame structure of the standard MPCP message illustrated in FIG. 4 with the inner structure of the security capability field;

[0055] FIG. 6 is a flowchart illustrating steps for distributing a key through an ONU using a key related MPCP message defined to set a security channel in an EPON according to an embodiment of the present invention;

[0056] FIG. 7 is a flowchart showing steps for providing a key distribution through an OLT using a key related MPCP

message defined for setting a security channel in an EPON according to an embodiment of the present invention; and

[0057] FIG. 8 illustrates various types of key distribution related MPCP message described in FIGS. 6 and 7 according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0058] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Like reference numerals denote like elements in different drawings. Detailed description of the known functions and configuration, which may be deviated from the concerned scope and spirit of the present invention, will be omitted.

[0059] FIG. 4 is a flowchart of a method of registering and negotiating a security capability between an OLT and ONUs to set a security channel in an EPON according to an embodiment of the present invention. Particularly, FIG. 4 illustrates steps for registering ONUs and negotiating the security capability at the same time by adding a 12 bits security capability field in a MPCP message defined in a standardized IEEE802.3ah EPON.

[0060] As shown in FIG. 4, when a discovery window is opened, the OLT 200 transmits a discovery gate message GATE to discover the ONUs similar to the standardized method at step S110. Since the OLT 200 does not know the existence of the ONUs, a multicast address dest_address-multicast is used as a destination address. The discovery gate message GATE includes the 6-byte timeslot allocation information GRANT for a new ONU 100 to respond to the discovery gate message GATE, the capability OLT capability, and the 12-byte security capability information OLT Security Capabilities to set a security function to the ONU 100. The 12-byte security capability information (OLT Security Capabilities) includes an encryption channel type, an encryption algorithm type, an encryption mode per frame type, and other parameters.

[0061] The newly defined ONU 100, which receives the discovery gate message GATE, sets an upstream transmission time using the timeslot allocation information. At the transmission time, the ONU 100 requests an intended number of IDs of physical layers (PHY ID) using a register request message REGISTER_REQUEST at step S130. At this time, the register request message REGISTER_REQUEST uses a source point MAC address of the ONU 100. The register request message REGISTER_REQUEST includes capabilities of the physical layer ID (PHY ID capa.), capability of the ONU 100 (ONU capa.), capability of the OLT 200 (echo of OLT capa.), and security capability of the OLT 200 (echo of OLT Security Capabilities).

[0062] Meanwhile, the ONU 100 checks whether the security capability information received from the OLT 200 can be set. If the ONU 100 can set the OLT security capability information requested by the OLT 200, the ONU 100 sets the security capability of the OLT 200 at step S120. Also, using the register request message REGISTER_REQUEST, the ONU 100 transmits again to the OLT 200 the OLT security capability information that has requested by the OLT 200, thereby completing the security agreement at step S130.

[0063] If the security capability field of the register request message REGISTER_REQUEST includes the security capability information of the OLT 200, the OLT 200 determines that the ONU 100 normally satisfies the security setting request for the OLT 200. Then, the security capability negotiation with the ONU 100 is completed.

[0064] If the ONU 100 cannot set the OLT security capability information requested by the OLT 200 at step S140, the ONU 100 transmits the security capability information of the ONU 100 to the OLT 200 using the register request message REGISTER_REQUEST at step S150. If the ONU 100 does not provide the security function, the ONU security capability information is not transmitted.

[0065] After receiving the register request message REGISTER_REQUEST including the ONU security capability information that has transmitted from the ONU 100 at step S150, the OLT 200 determines that the ONU 100 does not satisfy the security setting request made by the OLT 200, and thus, the OLT 200 checks whether the OLT 200 can accept the security capability requested by the ONU 100.

[0066] If the OLT 200 can set the security capability of the ONU 100 at step S160, the OLT 200 sets the security capability corresponding to the ONU security capability information. At step S170, the OLT 200 transmits to the ONU 100 information about the security capability of the ONU 100 that is set by the OLT 200 using a register message REGISTER. Then, the security capability negotiation of the OLT 200 with the ONU 100 is completed. At this time, the OLT 200 transmits the ONU security capability information to the ONU 100 along with allocating the IDs of the physical layers to the source point MAC address of the ONU 100.

[0067] If the OLT 200 cannot set the security capability of the ONU 100 at step S180, the OLT 200 transmits a register message that does not include the security capability information to the ONU 100. As a result, at step S190, the security function is not provided to the ONU 100.

[0068] The OLT 200 transmits the register message REGISTER that instructs the allocation of the IDs of the physical layers to the ONU 100 in the step S170. Afterwards, at step S210, the OLT 200 transmits a general gate message GATE to the ONU 100 to provide an upstream transmission of the ONU 100. The general gate message GATE includes information on allocation of a transmission time for a register acknowledgement message REGISTER_ACK that verifies whether the ONU 100 normally receives the transmitted register message REGISTER in the operation of S170, and the IDs of the physical layers are allocated.

[0069] When the ONU 100 receives the transmitted register message REGISTER in the operation of S170, the ONU 100 stores the IDs of the physical layers included in this register message REGISTER into a register. If the ONU security capability information is included in the received register message REGISTER, the ONU 100 determines that the OLT 200 sets the security capability of the ONU 100 according to the provided ONU security capability information and completes the security capability negotiation. If the register message REGISTER, which is transmitted at the step S190, does not include the security capability information, the ONU 100 determines that the OLT 200 does not set the security capability. As a result, the security function is not applied.

[0070] At step S220, when the ONU 100 receives the general gate message GATE that is transmitted at the step S210, the ONU 200 sets an upstream transmission time, and at the upstream transmission time, transmits the register acknowledgement message REGISTER_ACK to the OLT 200 as a response to the receipt of the IDs of the physical layers.

[0071] After receiving the register acknowledgement REGISTER_ACK, the OLT 200 determines that the IDs of the physical layers are allocated normally to the ONU 100, and the OLT 200 completes the automatic registration of the ONU 100 and generates a channel at step S230.

[0072] FIG. 5 illustrates a frame structure of the standard MPCP message illustrated in FIG. 4 with the inner structure of the security capability field.

[0073] As shown, the standard MPCP message 300 is composed of 64 bytes. The 14-byte of header information 300 includes a 6-byte destination address, a 6-byte source address and a 2-byte MPCP message Ethernet type information. A 2-byte OP CODE 301 is used as an identifier of the MPCP message. A 4-byte time stamp 302 is used as a transmission time unit. A 40-byte parameter list 303 includes different information for each MPCP message. Particularly, the 40-byte parameter list 303 includes the 12-byte security capability field 304 as illustrated in the embodiment of the present invention.

[0074] The 12-byte security capability field 304 is configured with various channel information including a secure connectivity association (CA) information 306 and a secure channel (SC) association information 307, a security algorithm type 308, a security mode per frame type 309, control parameters 310 (e.g. a security mode per security function), an almost PN expire value 311, and a PN change value 312.

[0075] The 4-byte CA information 306 denotes security algorithm types that can be implemented between the OLT 200 and the ONU 100 and provides four types of the security algorithms in bit maps. More specifically, when the OLT 200 and the ONU 100 use substantially the same algorithm, the CA information is set. Currently, a GCM-AES algorithm can be set according to the IEEE802.1ae standard. In the present embodiment, if a bit C 313 has a value of '1', the bit C 313 represents that the GCM-AES algorithm is used. On the other hand, '0' of the bit C 313 denotes that the GCM-AES algorithm is not used.

[0076] The 4-byte SC information 307 is used to indicate whether the security function is to be implemented for unicast and broadcast channels. Also, the 4-byte SC information indicates whether the security capability field 304 is for use in the OLT or ONU. More specifically, a bit U 314 represents a state of the security setting for the unicast channel, and a bit B 315 represents a state of the security information for the multicast channel. If a bit S 316 has a value of '1', the bit S 316 is indicative of the security capability information for use in the OLT. On the other hand, if the bit S 316 has a value of '0', the bit S 316 is indicative of the security capability information for the ONU.

[0077] The 1-byte security algorithm type information 308 is used to set an encryption mode between the OLT and the ONU. This usage for the encryption operation mode is illustrated in Table 1 below:

TABLE 1

Encryption mode (EM) bit	MODE
00	Authentication Encryption
01	Authentication Decryption
10	Authentication Generation
11	Authentication Check

[0078] Also, the 1-byte security mode per frame type information 309 is used to individually encode various types of frames transmitted from the EPON. That is, if a bit FT 318 has a value of '1', the encoding proceeds. On the other hand, the encoding does not proceed if the bit FT 318 has a value of '0'. Table 2 below illustrates this usage for the security mode per frame type.

TABLE 2

Bit FT	FT(2)	FT(1)	FT(0)
Frame Type	MPCP frame	OAM frame	Data frame

[0079] The 1-byte control parameter information 310 is used to activate or inactivate the internal security function. For instance, if a bit ED 319 has a value of '1', the internal security function is activated. On the other hand, if the bit ED 319 has a value of '0', the internal security function is inactivated. This functional control information is illustrated in Table 3 below.

TABLE 3

Bit ED	ED(2)	ED(1)	ED(0)
Function Type	Authentication check	Keyplay attack check	DoS attack check

[0080] The almost PN expire value 311 indicates a moment to request a key necessary for a next cycle after completing the present cycle. The 4-byte PN change value 312 indicates a moment to change the key (i.e., PN) after completing the present cycle. A 4-byte field check sequence (FCS) information 305 provides an error check function for the MPCP frame 3300.

[0081] FIG. 6 is a flowchart illustrating steps for distributing a key through an ONU using a key related MPCP message defined to set a security channel in an EPON according to an embodiment of the present invention.

[0082] As shown, the key distribution between the ONU 100 and the OLT 200 is performed after the security negotiation and automatic registration procedure described in FIG. 4 is completed. Therefore, the key distribution is applied to those ONUs completed with the security negotiation and automatic registration.

[0083] The key distribution procedure is performed as follows. The ONU 100 includes a CPU for the key distribution.

[0084] At step S410, the OLT 200 transmits a key request message KEY_REQUEST to the ONUs 100 completed with the security capability agreement. The key request message KEY_REQUEST requests an encryption key to be used in a

security channel. The key request message KEY_REQUEST can request the encryption key to all of the ONUs or a specific ONU 100. The key request message KEY_REQUEST provides a nonce used to make random encryption keys at the ONU 100.

[0085] When the ONU 100 receives the key request message KEY_REQUEST, the ONU 100 generates an encryption key using the nonce included in the key request message KEY_REQUEST at step S420. The ONU 100 transmits the generated encryption key message ENCRYPTION_Key to the OLT 200 at step S430. The ONU 100 activates a security mode at step S440. The encryption key message ENCRYPTION_Key transmitted to the OLT 200 is not encoded since other ONUs cannot see the encryption key message ENCRYPTION_Key without disconnecting the link due to the topological configuration characteristic of the EPON. One encryption key message ENCRYPTION_Key provides about 40 bytes of encryption key information at the maximum. The GCM-AES encryption algorithm standardized by the IEEE802.1ae uses about 24 bytes of an encryption parameter for each securing channel, and thus, one encryption parameter can be provided per one message. On the contrary, in case of using an AES encryption algorithm standardized by NIST, about 16 bytes of the encryption parameter are used for each security channel. Thus, about 2 encryption parameters can be provided per one message at the maximum.

[0086] Once the OLT 200 receives the encryption key message ENCRYPTION_Key, the OLT 200 stores the encryption parameters included in the parameter list into a key register and then, activates an encryption mode at step S450. The OLT 200 encodes a key register acknowledgment message KEY_REGISTER_ACK using the stored encryption key and transmits the key register acknowledgment message KEY_REGISTER_ACK to the ONU 100 thereafter at step S460.

[0087] The ONU 100 decodes the key register acknowledgment message KEY_REGISTER_ACK. If the decoded message is substantially the same as the encoded parameter of the ONU 100, the encryption mode of the ONU 100 is maintained at step S470, and if otherwise, the encryption mode is inactivated.

[0088] At step S480, the encryption modes of the OLT 200 and the ONU 100 are activated, completing the encryption setting. Afterwards, the ONU 100 and the OLT 200 provide the security function for the transmitted frames at step S490. At step S495, the OLT 200 transmits a key change time (or cycle) message KEY_CHANGE_TIME to the ONU 100 to renew a cycle of the distributed key.

[0089] FIG. 7 is a flowchart showing steps for providing a key distribution through an OLT using a key related MPCP message defined for setting a security channel in an EPON according to an embodiment of the present invention.

[0090] As shown in FIG. 7, the key distribution between the OLT 200 and the ONU 100 is performed after the completion of the automatic registration procedure illustrated in FIG. 4. The key distribution procedure is performed as follows. A CPU of the OLT 200 generates and distributes a key. Hence, the ONU 100 does not need to have a CPU to distribute the key.

[0091] At step S610, the ONU 100 transmits a key request message KEY_REQUEST that requests an encryption key

to be used in the security channel to the OLT 200 completed with the security capability agreement. The key request message KEY_REQUEST provides a nonce used to produce random encryption keys at the OLT 200.

[0092] After receiving the key request message KEY_REQUEST, the OLT 200 generates an encryption key using the nonce included in the key request message KEY_REQUEST at step S620. The OLT 200 transmits an encryption key message ENCRYPTION_KEY message that is encoded using a master key to the ONU 100 at step S630. Those downstream frames are likely to be exposed to other ONUs due to the topological configuration characteristic of the EPON, and thus, the encryption key message ENCRYPTION_KEY is transmitted after being encoded using the precedence setting master key of the OLT 200 and the ONU 100. The master key can be used regardless of the activation state of the encryption mode.

[0093] At step S640, the ONU 100 receives the encryption key message ENCRYPTION_KEY that has been encoded using the master key and then, decodes the encryption key message ENCRYPTION_KEY. If the decoding is successful, the encryption key is stored into a key register and the encryption mode is activated. If otherwise, the encryption key is not stored and the encryption mode is inactivated.

[0094] At step S650, the ONU 100 transmits a key register acknowledgement message KEY_REGISTER_ACK to the OLT 200 using the encryption key message ENCRYPTION_KEY received from the OLT 200.

[0095] At step S660, the OLT 200 decodes the encoded key register acknowledgement message KEY_REGISTER_ACK using the key of the ONU 100. If the decoding is successful, the activation state of the encryption mode is maintained. If otherwise, the encryption mode is inactivated.

[0096] At step S670, the security setting is completed as the encryption modes of the OLT 200 and the ONU 100 are activated. Afterwards, the OLT 200 and the ONU 100 provide the security function for the transmitted frames at step S680. Then, the ONU 100 transmits an encoded key change time message KEY_CHANGE_TIME that indicates a key change cycle to the OLT 200 at step S690.

[0097] FIG. 8 illustrates various types of key distribution-related MPCP message described in FIGS. 6 and 7 according to an embodiment of the present invention.

[0098] As illustrated, there are four types of the MPCP message associated with the key distribution. More specifically, a key request message KEY_REQUEST 600 requests an encryption key or parameters used in a security channel. An encryption key message ENCRYPTION_KEY 601 transmits the generated encryption key or parameters. A key register acknowledgement message KEY_REGISTER_ACK 602 is used as a response message to the encryption key message ENCRYPTION_KEY 601. A key change time message KEY_CHANGE_TIME 603 indicates a cycle of changing the key.

[0099] According to the present invention, the automatic registration of the ONUs can be achieved by the reciprocal security capability negotiation between the OLT and the corresponding ONU using the MPCP. Also, using various types of the MPCP messages that are newly defined for the key distribution allow effective providing of the key distribution function.

[0100] The above described method according to the present invention can be embodied as a program and stored on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can be thereafter read by the computer system. The computer readable recording medium includes a read-only memory (ROM), a random-access memory (RAM), a CD-ROM, a floppy disk, a hard disk, an optical magnetic disk, and carrier waves such as data transmission through the Internet. The computer-readable recording medium can also be distributed over network-coupled computer systems so that the computer-readable code is stored and executed in a distributed fashion. Also, functional programs, codes, and code segments for accomplishing the present invention can be easily construed by programmers skilled in the art to which the present invention pertains.

[0101] It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method for setting a security channel between an optical line terminator (OLT) and at least one optical network unit (ONU) in an Ethernet passive optical network (EPON), the method comprising the steps of:

- a) at the OLT, generating a channel by negotiating a reciprocal security capability with at least one of ONUs, which want to set a security channel in a discovery interval, using a multi-point control protocol (MPCP) message and various security capability information of the OLT and the ONU and automatically registering the ONU completed with the security capability negotiation;
- b) at the OLT, setting the security channel by distributing an encryption key for the security to the ONU making an agreement of the security capability negotiation among the ONUs that have been completed with the security capability negotiation and the automatic registration; and
- c) sharing a renewal point of the encryption key by transmitting a message indicative of a time to change the encryption key between the OLT and the ONU both completed with the encryption key distribution after the setting of the security channel.

2. The method of claim 1, wherein the step a) includes the steps of:

at the OLT, including the security capability information of the OLT into a discovery gate message and transmitting the discovery gate message to discover the ONU;

at the ONU, setting a security capability corresponding to the security capability of the OLT and transmitting to the OLT a register request message including the information of the security capability of the OLT if the ONU that has received the discovery gate message is able to accept the information of the security capability of the OLT;

- at the OLT, receiving the register request message, determining that the ONU has set the security capability according to the security capability of the OLT, and completing the security capability agreement with the ONU; and
- performing the automatic registration between the OLT and ONU both completed with the security capability negotiation and generating the channel.
3. The method of claim 1, wherein the step a) includes the steps of:
- at the OLT, including the security capability information of the OLT into a discovery gate message and transmitting the discovery gate message and used to discover the ONU;
 - at the ONU, transmitting to the OLT a register request message including information on the security capability of the ONU if the ONU that has received the discovery gate message is unable to accept the information of the security capability of the OLT;
 - at the OLT, setting a security capability corresponding to the information on the security capability of the ONU and transmitting to the ONU a register message including the information on the security capability of the ONU if the OLT is able to accept the information on the security capability of the ONU;
 - at the ONU, receiving the register message, determining that the OLT has set the security capability according to the information on the security capability of the ONU, and completing the security capability agreement with the OLT;
 - at the OLT, transmitting a general gate message to the ONU;
 - at the ONU, receiving the general gate message and transmitting a register acknowledgement message to the OLT;
 - at the OLT, receiving the register acknowledgement message and completing the security capability agreement with the ONU; and
 - performing the automatic registration between the OLT and ONU both completed with the security capability agreement and generating the channel.
4. The method of claim 3, wherein the step a) further includes the step of, at the OLT, transmitting a register message that does not include the various security capability information of the OLT and the ONU from the OLT to the ONU if the OLT is unable to accept the information on the security capability of the ONU.
5. The method of claim 1, wherein the step b) includes the steps of:
- at the OLT, transmitting a key request message that requests the encryption key for the security channel to the ONU completed with the security capability agreement;
 - at the ONU, generating an encryption key message using the key request message, transmitting the encryption key message to the OLT and activating an encryption mode; and
 - at the OLT, receiving the encryption key message, activating an encryption mode, encoding a key register acknowledgement message using a stored encryption key, and transmitting the encoded key register acknowledgement to the ONU.
6. The method of claim 5, wherein the step b) further including the steps of:
- at the ONU, receiving the key register acknowledgement message and decoding the received key register acknowledgement message;
 - maintaining the activation state of the encryption mode if the decoded key register acknowledgement message and the encryption key message are substantially the same; and
 - changing the encryption mode from the activation state to an inactivation state if the decoded key register acknowledgement message and the encryption key message are not the same.
7. The method of claim 1, wherein the step b) includes the steps of:
- at the ONU that has completed with the security capability negotiation, transmitting a key request message that requests the encryption key for the security channel to the OLT;
 - at the OLT, receiving the key request message, generating an encryption key message using the key request message, encoding the encryption key message using a master key, and transmitting the encryption key message to the ONU; and
 - at the ONU, receiving the encryption key message and selectively activating or deactivating the encryption mode according to the result whether the ONU decodes the received encryption key message successfully or not; and
 - at the ONU, encoding a key register acknowledgement message using the received encryption key and transmitting the key register acknowledgement message to the OLT.
8. The method of claim 7, further including the step of selectively activating or deactivating the encryption mode according to the result whether the OLT that has received the key register acknowledgement message decodes successfully or not.
9. The method of claim 1, wherein the MPCP message includes over-header information, an OPCODE, a time stamp, a parameter list including the security capability information, and field check sequence information.
10. The method of claim 9, wherein the security capability information includes secure connectivity association information, secure channel association information, security algorithm type information, security mode per frame type information, control parameter information including an encryption function activation mode, almost PN expire value information, and PN change value information.
11. The method of claim 10, wherein in the secure connectivity association information, a lower 1 bit is indicative of usage of a GCM_AES algorithm used in an IEEE802.1ae.
12. The method of claim 10, wherein in the secure connectivity association information, lower 2 bits are indicative of a security function setting for a logic link of a unicast

18. The structure of claim 17, wherein the security capabilities information includes secure connectivity association information, secure channel association information, security algorithm type information, security mode per frame type information, control parameter information including an encryption function activation mode, almost PN expiry value information, and PN change value information.

19. The method of claim 18, wherein in the secure connectivity association information, a lower 1 bit is indicative of usage of a COMBES algorithm used in an IEEE802.1ae.

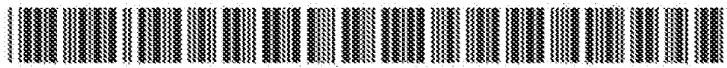
20. The method of claim 18, wherein in the secure connectivity association information, lower 2 bits are indicative of a security function setting for a logic link of a multicast and a broadcast, and a third bit indicates whether the security capability information is for the COT or the ONU.

21. The method of claim 18, wherein in the security algorithm type information, lower 2 bits set an encryption operation mode between the COT and the ONU.

22. The method of claim 18, wherein in the security mode per frame type information, lower 3 bits indicate whether the encryption is applied individually for different types of frames transmitted in the EPON.

23. The method of claim 18, wherein in the control parameter information including the encryption function activation mode, lower 3 bits set an activation or function state of an internal security function.

24. The method of claim 18, wherein the almost PN expiry value information and the PN change value information set a time for requesting the encryption key for a next cycle and a time to change the encryption key for the next cycle.



US 20060031936A1

(19) **United States**(12) **Patent Application Publication**

Nelson et al.

(10) **Pub. No.: US 2006/0031936 A1**(45) **Pub. Date:****Feb. 9, 2006**(54) **ENCRYPTION SECURITY IN A NETWORK SYSTEM****Publication Classification**(75) **Inventors:** David B. Nelson, Derry, NH (US);
Richard W. Graham, Derry, NH (US)(51) **Int. Cl.**
G06F 12/14 (2006.01)
(52) **U.S. Cl.** 726/23(57) **ABSTRACT**

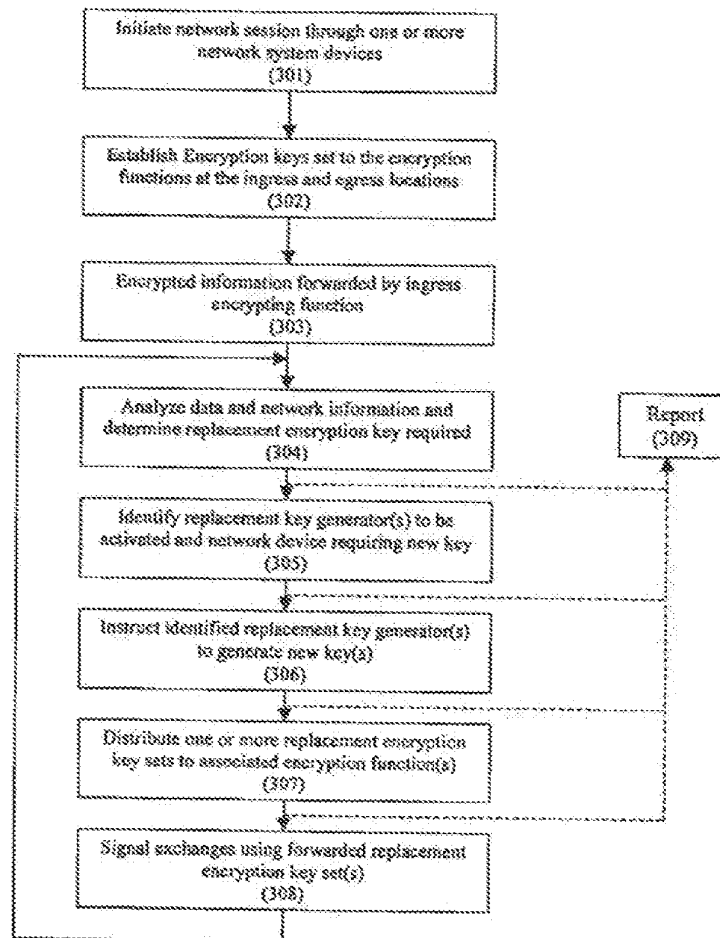
Correspondence Address:

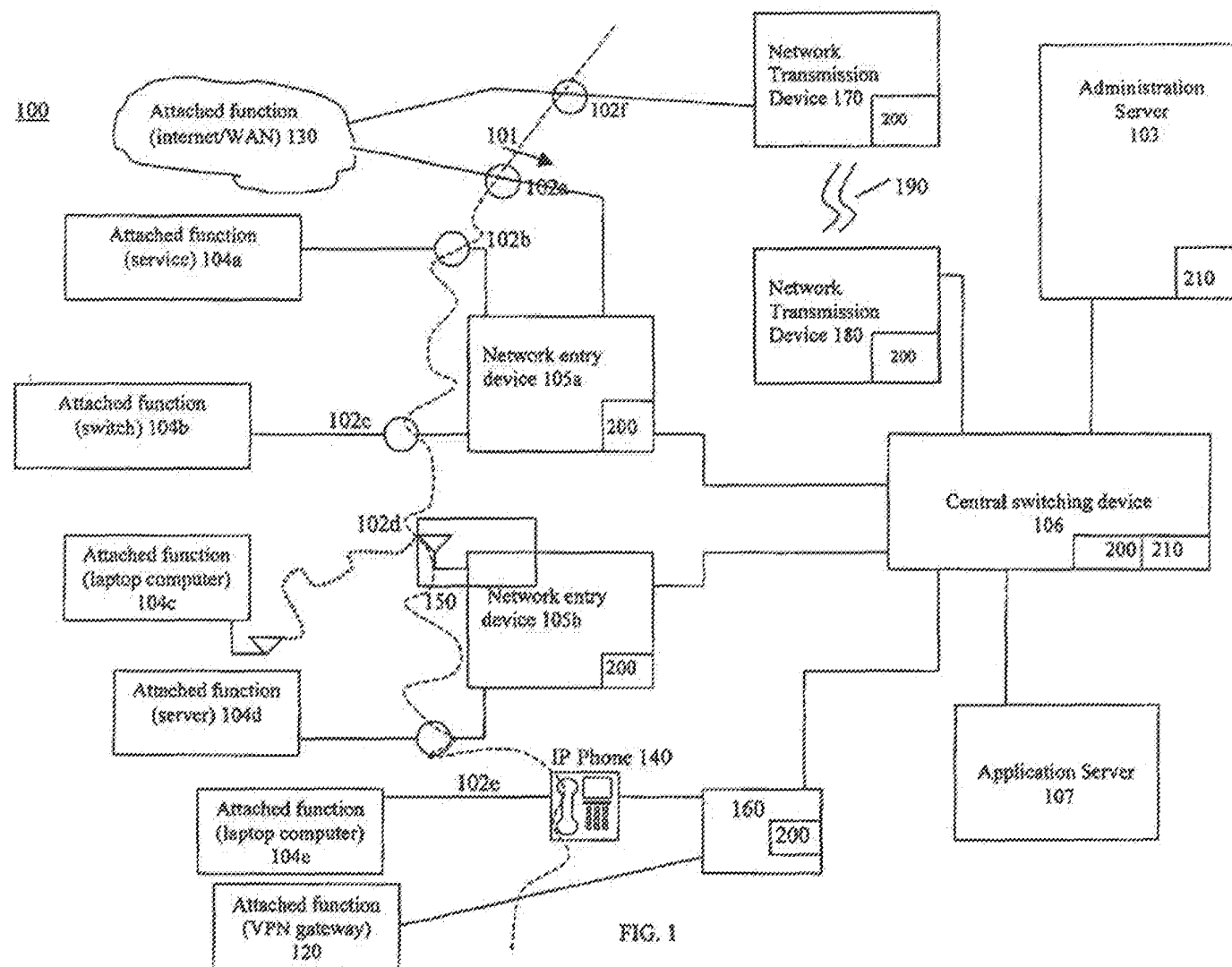
CHRIS A. CASEIRO
VERRILL DANA, LLP
ONE PORTLAND SQUARE
PORTLAND, ME 04112-0586 (US)

A system and method for enhancing the security of signal exchanges in a network system. The system and method include a process and means for generating one or more replacement encryption key sets based on information and events. The information that may cause the generation of a replacement encryption key set includes, but is not limited to, a specified period of time, the level and/or type of signal traffic, and the signal transmission protocol and the amount of data sent. A key manager function initiates the replacement encryption key process based on the information. The replacement encryption key set may be randomly or pseudo-randomly generated. Functions attached to the network system required to employ encryption key sets may have encryption key sets unique to them or shared with one or more other attached functions. The system and method may be employed in a wireless, wired, or mixed transmission medium environment.

(73) **Assignee:** Enterasys Networks, Inc., Andover, MA (US)(21) **Appl. No.:** 10/971,905(22) **Filed:** Oct. 22, 2004**Related U.S. Application Data**

(63) Continuation-in-part of application No. 10/116,447, filed on Apr. 4, 2002.





Network Device

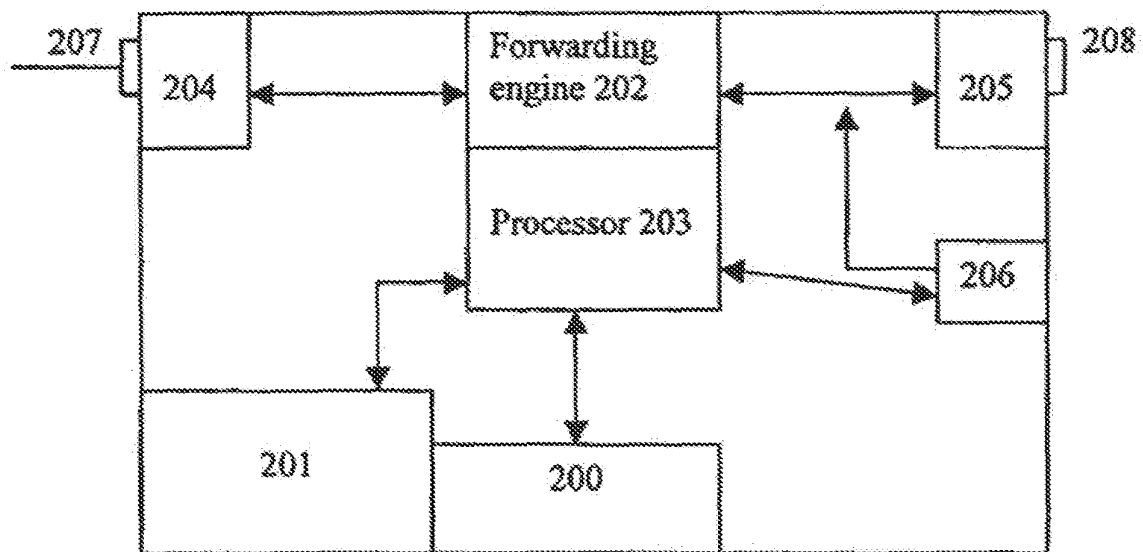


FIG. 2

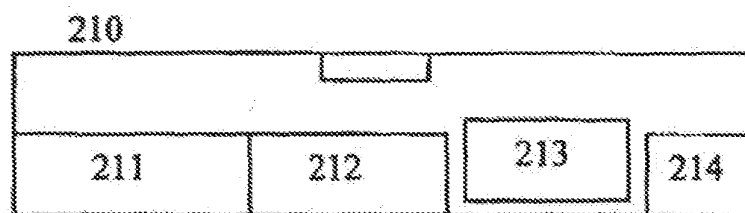


FIG. 3

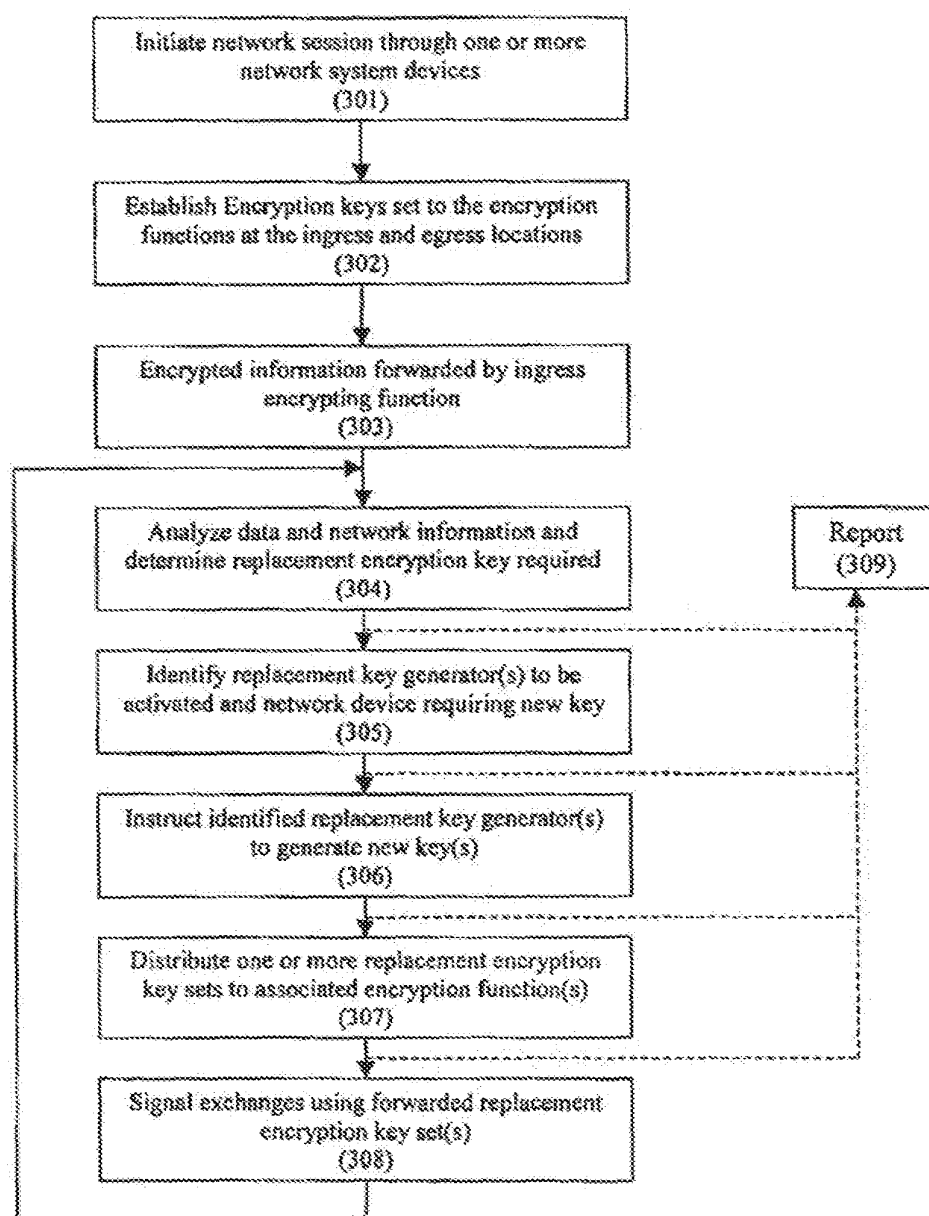


FIG. 4

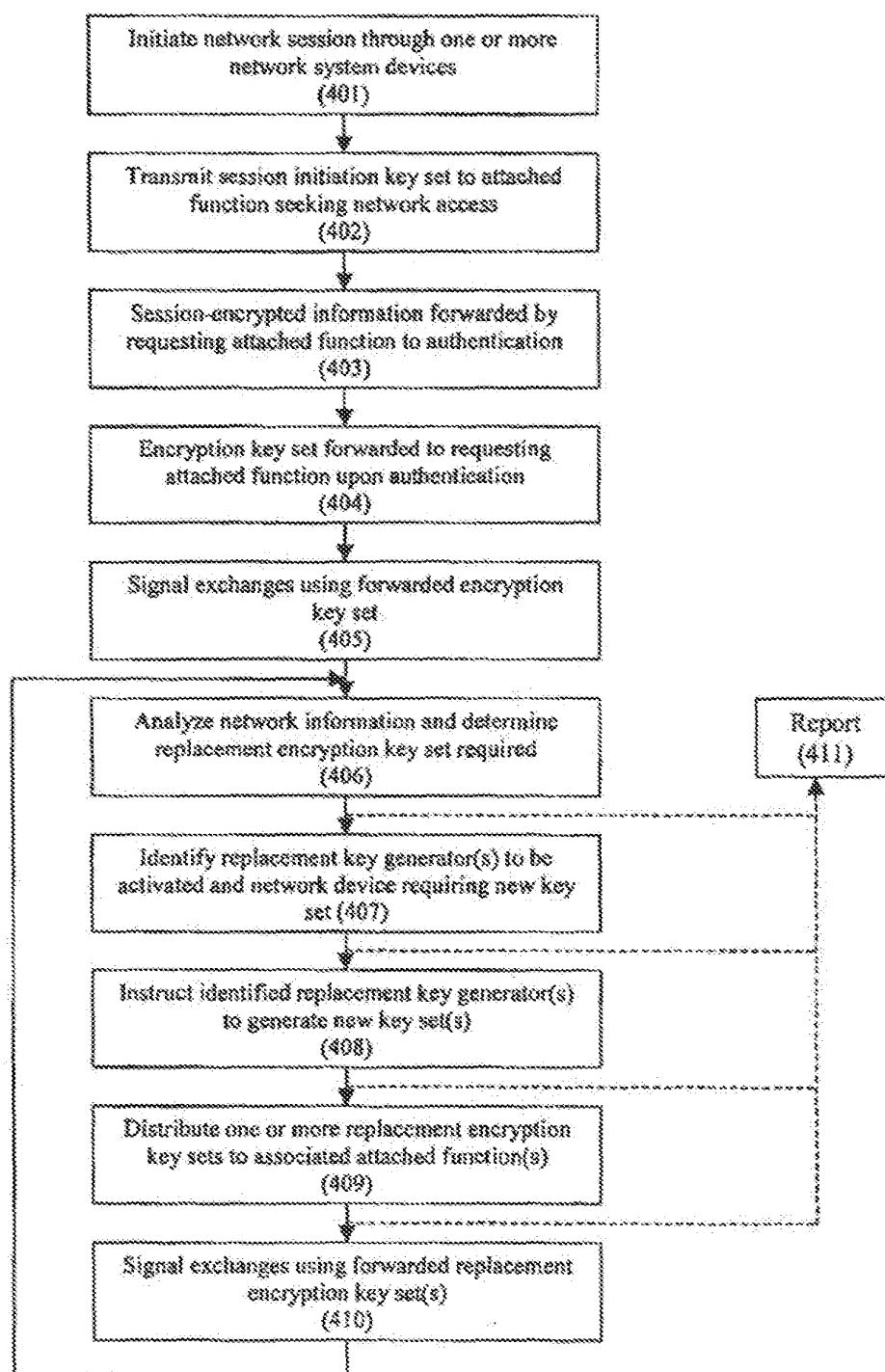


FIG. 5

ENCRYPTION SECURITY IN A NETWORK SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation-in-part of co-pending U.S. patent application Ser. No. 10/116,447, filed Apr. 4, 2002, entitled **UA SYSTEM AND METHOD TO PROVIDE ENHANCED SECURITY IN A WIRELESS LOCAL AREA NETWORK SYSTEM** owned by a common assignee. The content of that application is incorporated herein by reference and priority is claimed therein.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to systems and methods for enhancing the security of signal exchanges in network systems. More particularly, the present invention relates to systems and methods for encrypting such exchanges.

[0004] 2. Description of the Prior Art

[0005] Interconnected computing systems form the basis of a network. A network permits communication or signal exchange among computing systems of a common group in some selectable way. The interconnection of those computing systems, as well as the devices that regulate and facilitate the exchange among the systems, represent a network. Further, networks may be interconnected together to establish internetworks. For purposes of the description of the present invention, the devices and functions that establish the interconnection represent the network infrastructure. The users, computing devices and the like that use that network infrastructure to communicate are referred to herein as attached functions and will be further defined. The combination of the attached functions and the network infrastructure will be referred to as a network system.

[0006] Presently, access to applications, files, databases, programs, and other capabilities associated with the entirety of a discrete network is restricted primarily based on the identity of the user and/or the network attached function. For the purpose of the description of the present invention, a "user" is a human being who interfaces via a computing device with the services associated with a network. For purposes of further clarity, a "network attached function" or an "attached function" may be a user connected to the network through a computing device and a network interface device, an attached device connected to the network, a function using the services of or providing services to the network, or an application associated with an attached device. Upon authentication or other form of confirmation of the offered attached function identity, the attached function may access network services at the level permitted for that identification. For purposes of the present description, "network services" include, but are not limited to, access, data transport service, Quality of Service (QoS) capabilities, bandwidth, priority, computer programs, applications, databases, files, and network and server control systems that attached functions may use, communicate across or with manipulate for the purpose of conducting the business of the enterprise employing the network as an asset.

[0007] A network session is the establishment of an association between an attached function and one or more

network services through the network infrastructure. It is to be understood, however, that a network system may be embodied in the combination or interrelation between one or more attached functions and one or more network infrastructure devices. At the outset of a network session, often in relation to the authentication of the entity requesting the session, an association is created between the attached function and/or one or more network infrastructure devices and one or more network services, constrained by one or more policies enforced based on policy enforcement rules carried out by one or more devices of the network infrastructure.

[0008] The process by which the various computing systems of a network or internetwork communicate is regulated by agreed-upon signal exchange standards and protocols embodied in network devices, interface cards, circuitry and software. Such standards and protocols were borne out of the need and desire to provide interoperability among the array of computing systems available from a plurality of suppliers. Two organizations that have been substantially responsible for signal exchange standardization are the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF). In particular, the IEEE standards for internetwork operability have been established, or are in the process of being established, under the purview of the 802 committee on Local Area Networks (LANs) and Metropolitan Area Networks (MANs).

[0009] Among others, the IETF has established a protocol to secure signal transmissions at Layer 4 of the Open Systems Interconnection (OSI). The Transport Layer Security (TLS) protocol defined by the IETF is based upon the Secure Sockets Layer (SSL) protocol and involves the encryption of transport layer transmissions based on a public key-private key exchange. Specifically, an end user contacts a service provider to gain access to the Internet. The answering server sends a public key to the user's browser that in turn generates a random private key that is employed for the remainder of the secured Internet session. A break in the signal exchange between the server and the browser requires re-initialization of the TLS protocol.

[0010] In another example of a standardized technique to enhance network session security, IEEE standard 802.1X is designed to improve network security. It establishes a framework for network authentication of a user seeking to connect to a particular network and access programs associated with that network, and for distribution of encryption keys for use at Layer 2 of the OSI. When a user initiates connection to the network through a network system device, the device, such as a switch, a router, or a wireless access point, for example, initially only forwards user request information, including identity information pursuant to an authentication protocol, such as the Extensible Authentication Protocol (EAP), to network management. All other communication activities are blocked during the authentication process. An authentication server of the network then resolves the user's network access permissions, if any, and forwards an accept/reject message to the network access device. The network access device then either authorizes access or it blocks access for the requesting user. IEEE standard 802.1X is applicable to wired and wireless network connections.

[0011] IEEE standard 802.11 is directed to wireless LAN (WLAN) standards and Layer 2 of the OSI in particular. The

standard establishes a framework for the bands of radio signal propagation to enable bit transmission rates substantially compatible with existing expectations of network signal exchange rates. Whereas 802.1X defines network access authentication regardless of signal transmission medium, 802.11 is specifically directed to transmission standards in a wireless environment. Neither specifically addresses the security of signal exchanges in a wired or wireless environment once network access has been established.

[0012] An IETF-based method for securing signal exchanges across otherwise unsecured public network systems—such as the internet—is the Virtual Private Network (VPN). A VPN is a network arrangement constructed from both public and private devices. Such interconnection are generally established by enterprises having separated offices or locations that must be interconnected across public infrastructures. A VPN permits the sharing of private information across the public infrastructure through the encryption of the signal exchanges. The encryption methodology is standardized to produce what is generally referred to as a tunnel. That is, the encryption creates a what is intended to be a hardened tunnel through which the VPN signal exchanges pass encased by the standardized signal exchange protocols associated with the public infrastructure.

[0013] Currently, there are four different protocols generally employed in the creation of these VPN tunnels. They are Point-to-Point Tunneling Protocol (PPTP), Layer-2 Forwarding (L2F), Layer-2 Tunneling Protocol (L2TP), and Internet Protocol Security Protocol (IPSec). IPSec tends to be directed to LAN-to-LAN exchanges while the other protocols tend to be employed for dial-up exchanges. IPSec employs encryption keys to secure data and/or packet headers. Public/private encryption keys are exchanged between communicating devices through the Internet Key Exchange (IKE) standard. At the start of a network session, the keys are exchanged to establish the tunnel. The same keys are used throughout the course of the session to encrypt the signals exchanged. Unfortunately, with sufficient time, signal exchange volume, applied computing power and/or because of flaws in the encryption algorithms or implementations, it has been determined that the encrypted signals can be compromised.

[0014] It is known that wireless communications may be more susceptible to interception than signal transmissions on wired or fiber media. Nevertheless, signal transmissions in wired or fiber environments may also be susceptible to interception. Intercepted signals may be used for unauthorized gathering of information as well as unauthorized access to the network. As a result of those concerns, wireless network communications, like VPN communications, are preferably encrypted. It is widely believed that the encryption of a wireless transmission equates to the security associated with a wired network for which physical security mechanisms are possible.

[0015] The Wired Equivalent Privacy (WEP) algorithm provides under IEEE 802.11 the standardized wireless encryption method. WEP involves the use of a secret or private key that is shared among one or more mobile computer systems and an access point that is wired to a network. The key, a string of bits, is combined with readable data in a defined mathematically determined manner to

generate ciphered data. In particular, WEP uses the RC4 algorithm to generate a pseudo-random key stream that is combined with the data to generate encrypted data packets. The receiver, having the same key and algorithm, simply performs the inverse same mathematical function on the cipher stream to reproduce the readable data. In order to avoid duplicative ciphering, which aids crypto analysis, WEP further employs an initialization vector (IV), or public key, added to the secret key, prior to ciphering, to minimize re-use of the same effective cipher key. The IV is currently a 24-bit field that transmits in clear text. With sufficient traffic on the WLAN, the IV and corresponding private portion of the WEP key can be detected by crypto analysis, decrypted, and the network and its traffic exposed and subject to compromise.

[0016] Therefore, what is needed is an improved system and method for securing signal exchanges in wired and wireless network environments. Further, what is needed is such a system and method that increases the difficulty of compromising the encryption of signal exchanges throughout a network session.

SUMMARY OF THE INVENTION

[0017] It is an object of the present invention to enhance the security of a network session through the generation of one or more replacement encryption keys and using such one or more replacement encryption keys to replace one or more existing keys during the network session. It is also an object of the invention to enable the enhancement to be employed in a wired or a wireless exchange, provided the encryption complies with existing exchange protocols including, but not limited to, wired LAN, MAN and WAN and wireless standards. These and other objects are met by providing the improved security at the point where an attached function and a network infrastructure device exchange signals, where two or more network infrastructure devices exchange signals, or where two attached functions exchange signals. In particular, one or more replacement encryption keys are generated and, during the course of the network session, the one or more replacement keys are used to replace one or more of the existing keys used to encrypt the signal exchanges of the session.

[0018] The present invention includes a method for enhancing the security of a network including one or more network infrastructure devices capable of exchanging messages. The method includes the steps of generating a plurality of encryption keys, encrypting some or all of the messages between two or more of the network infrastructure devices, or within one or more of the network infrastructure devices capable of exchanging messages across functions within the device, with one or more of the plurality of encryption keys, and in the course of the message exchanges, replacing one or more of the one or more encryption keys with one or more replacement encryption keys. In one alternative embodiment of the invention, the steps performed include generating a plurality of encryption keys for use in encrypting message exchanges between the one or more attached functions and the network, using the plurality of encryption keys in the message exchanges between the one or more network access devices and the one or more attached functions, generating one or more replacement encryption keys, and during the session, replacing one or more of the plurality of encryption keys with the one or

more replacement encryption keys at non-regular intervals. In another alternative embodiment of the invention, the method includes the steps of generating a plurality of encryption keys for use in encrypting messages between the one or more network access devices and one or more attached functions, encrypting some or all of the messages with one or more of the plurality of encryption keys, and in the course of exchanging messages with the one or more attached functions, without authenticating, transmitting to the one or more attached functions one or more replacement encryption keys to replace one or more of the one or more encryption keys. The plurality of encryption keys and the one or more replacement encryption keys may be randomly generated. Optionally, at least one of the one or more network access devices generates and transmits the plurality of encryption keys and the one or more replacement encryption keys.

[0019] In one form of the invention, at least two of the plurality of encryption keys is unique to each device or attached function including the encryption function. In another form of the invention, at least one of the plurality of encryption keys is shared among all encryption functions. The plurality of encryption keys may be replaced as a function of the number of encrypted messages, as a function of the amount of information exchanged during the session, or they may be replaced randomly. The method of the invention further includes the option of replacing one or more of the one or more replacement encryption keys during the session, and repeating that step as desired. The basis for generating and distributing replacement encryption keys may be different from one replacement cycle to another. In a form of the invention, a first one of the plurality of encryption keys is designated a transmit key and a second one of the plurality of encryption keys is designated a receive key.

[0020] In order to effect efficient replacement of one or more existing keys with one or more generated replacement keys, at least one of the plurality of encryption keys may be designated for multicast transmissions and/or broadcast transmissions. Further, one or more of the encryption keys may be associated with a transmission protocol or a set of transmission protocols. Optionally, at least one of the plurality of encryption keys may be retained rather than replaced when others of the plurality of encryption keys are replaced. The retained encryption key or keys may be replaced with a second set of replacement encryption keys, wherein at least one of the second set of replacement encryption keys is a second retained encryption key that is not replaced when the one or more replacement encryption keys is replaced. The network device used to generate and transmit one or more replacement keys, or to transmit one or more replacement keys generated by another network system device may be a wireless access point, a local area network router, a wide area network router, a VPN appliance, or a switch, but is not limited thereto. The transmission of the one or more replacement keys may take place over a wired, including optical cabling, a wireless transmission medium, or a combination of the two.

[0021] The present invention is effective in the context of existing standards-based networks in that it contemplates the initial security features associated with initial access to the network by an attached function. For example, preliminary network authentication communication security keys may

first be used to authenticate the attached function to the network. Thereafter, the replacement key generation process enhances the security of the ongoing network session by replacing originally provided keys in a manner that may be random and that may be done as specified conditions are met. That is, key replacement may be programmed as a function of specified conditions including, for example, network perceived threat level, location of device or transmission apparatus and cabling or aggregation of signals, preferably ahead of any then-existing crypto analysis attack capabilities. It is anticipated that an event which might cause a more rapid tuning of the changing on the keys would be the advancement or discovery of hacker techniques or capabilities to more quickly decipher the data stream. The invention also uses the changing of the keys to improve capabilities of systems with time, performance and cost tradeoffs which implement less robust encryption techniques. Its use is expected to improve security for VPN and tunneling implementations and configurations where the tunnel may provide a secure transport but users of the system may not be authenticated. Initial authentication of devices may also be done manually or in some administration or trusted user defined method.

[0022] The details of one or more examples related to the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from any appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] FIG. 1 is a simplified diagrammatic block representation of an example network system with the enhanced security system of the present invention.

[0024] FIG. 2 is a simplified block representation of a network infrastructure device including the replacement encryption key generator of the present invention.

[0025] FIG. 3 is a simplified block representation of a key manager function of the present invention.

[0026] FIG. 4 is a flow diagram of a first embodiment of the process of the present invention for enhancing network system security.

[0027] FIG. 5 is a flow diagram of a second embodiment of the process of the present invention for enhancing network system security.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT OF THE INVENTION

[0028] The present invention is a system and related method to enhance the security of a network system through the replacement of one or more encryption keys in the course of a network session. Referring to FIG. 1, a representation of a network system 100 incorporating the capability of the enhanced security system of the present invention operates and provides network services to attached functions according to policies and policy enforcement rules to devices of a network infrastructure 101 through which the attached functions access and use services of the network system 100. Network system 100 includes the network infrastructure 101 and one or more attached functions connected to or connectable to the network infrastructure 101. The network

infrastructure 101 includes multiple switching devices, routing devices, firewalls, Intrusion Detection Systems, wired and wireless access points, Metropolitan Area Networks (MANs), WANs, VPN appliances, and internet connectivity interconnected to one another and connectable to the attached functions by way of connection points (e.g., 102a-f). The network infrastructure 101 includes such devices having forwarding functionality for the purpose of accessing and using network services.

[0029] The network infrastructure 101 may also include network transmission devices, shown in FIG. 1 and identified herein as devices 170 and 180. The network transmission devices 170 and 180 may be bridge devices that enable signal exchange at selectable layers of the OSI model at relatively high throughput. Device 170 is shown as a link between an external attached function, in this case the internet, and device 180. Device 180 is shown as connected to central switching device 106. It is to be understood that other sorts of transmission devices with other types of connections within and outside of the network infrastructure 101 may be embodied in the network system 100 and may be suitable for the encryption system of the present invention. Either or both of network transmission devices 170 and 180 may be wireless transmit/receive devices for signal exchanges across open spaces that may be susceptible to signal interception, such as between buildings of a campus. Such devices may not be protectable by current VPN security means. The present invention provides a means for establishing a secure exchange link 190 for these wireless exchanges. It is to be noted that such exchanges are ordinarily not subject to attached function authentication and are better thought of as part of the infrastructure links which are expected to have higher security and privacy than cleartext protocols on laser, infrared, RF or other open or assessable links, including some wired links. It is to be noted that the link 190 may also be a wire link spanning a location that may not be sufficiently secured from physical intrusion efforts.

[0030] A security enhancement system of the present invention includes a replacement encryption key generator 200 and a replacement key manager function 210. The replacement encryption key generator 200 generates replacement encryption keys by instruction from the replacement key manager function 210 and forwards the generated replacement encryption keys to network system devices, including attached functions. Each replacement encryption key generator 200 is preferably a random or pseudo-random number generator of the type known to those skilled in the art; however, in the process of generating replacement encryption keys, it preferably avoids repeating sequences and to avoid any known weak keys with respect to existing encryption algorithms.

[0031] The replacement key manager function 210 implements replacement key generation by the generator 200 by instruction to the generator 200 based on information. The key manager function 210 includes at least an analysis function to analyze network information to determine whether that information includes one or more conditions, events, occurrences, etc. ("triggers") for the purpose of implementing one or more encryption key replacements. The replacement key manager function 210 further includes an implementation function to signal to specific replacement encryption key generators 200 to proceed with generation and key forwarding.

[0032] Continuing with reference to FIG. 1, an attached function is external to infrastructure 101 and forms part of network system 100. Examples of attached functions 104a-104e are represented in FIG. 1, and may be any of the types of attached functions previously identified. Network infrastructure entry devices 105a-b, 140, and 160 of infrastructure 101 provide the means by which the attached functions connect or attach to the infrastructure 101. Alternative entry means may be used as noted in the following paragraph. A network entry device can include and/or be associated with a wireless access point 150. For wireless connection of an attached function to the infrastructure 101, the wireless access point 150 can be an individual device external or internal to the network entry device 105b. For the purpose of illustrating the response system of the present invention, each of the network entry devices except phone 140 includes the replacement encryption key generator 200. It is to be noted that a phone may include a replacement encryption key generator; however, that is not shown in FIG. 1. The network system 100 may include other network devices without a replacement encryption key generator 200. One or more centralized network infrastructure devices may include a replacement encryption key generator 200. Further, there may be a combination of network entry and centralized forwarding devices having the replacement encryption key generator 200 of the present invention. It is also to be noted that a replacement encryption key generator 200 may be included as part of one or more attached functions.

[0033] One or more central forwarding devices, represented by central switching device 106, enable the interconnection of a plurality of network entry devices, such as devices 105a-b and 160, as well as access to network services, such as administration server 103 or an application server 107. It is to be understood that a central forwarding device, or an entry forwarding device, is not limited only to switches as that term is traditionally understood. Instead, the forwarding device may be any device capable of forwarding signals through the network infrastructure pursuant to forwarding protocols. The central switching device 106 enables the interconnection of the network infrastructure 101 to attached functions that include VPNs (represented by VPN gateway device 120) and WANs (represented by internet cloud 130) as well as Internet Protocol (IP) telephones (represented by telephone 140). It is to be understood that the IP telephone 140 may also perform as a network entry device for the purpose of connecting an attached function, such as a laptop computer, to the network infrastructure 101.

[0034] One or more devices of the network infrastructure 101 include the replacement encryption key generators 200 of the security enhancement system of the present invention. The replacement encryption key generator 200 may be established in hardware and/or software (e.g., a function embodied in an application executing on one or more devices of the network infrastructure 101) to implement replacement encryption key generation. The particular network device on which the replacement encryption key generator 200 resides may vary from manufacturer to manufacturer. A network device may also be a port or set of ports, an interface or a set of interfaces.

[0035] As illustrated in FIGS. 2 and 3, the security enhancement system of the present invention includes several functions and elements as briefly described above. It is to be noted that all functions and elements may be embodied

in one or more devices of the network 100. However, the replacement encryption generator 200 of FIG. 2 will preferably be embodied in one or more devices of the network infrastructure 101 including, for example, the network entry device 105a, the centralized switching device 106, or the network transmission device 170. The key manager function 210 of FIG. 3 may be embodied in one or more devices of the network infrastructure 101 including, for example, the administration server 103, or the centralized switching device 106. However, it is to be noted that there may be a plurality of devices including the key manager function 210, each configured to initiate replacement encryption key generation and distribution for one or more network system devices.

[0036] A network device including the replacement encryption key generator 200 preferably also includes storage means 201, such as a database or a caching function, for storing replacement encryption key information and information regarding one or more attached functions associated with the particular network device to which such keys are distributed. The storage means 201 may be updated periodically or as a result of an event occurring anywhere in the network infrastructure 101. The storage means 201 may be a single database comprised of one or more updateable tables of information. A network device having forwarding functionality and with the replacement encryption key generator 200 includes a forwarding engine 202, a processor 203, an ingress port interface 204, an egress port interface 205, and a communication function 206.

[0037] As shown in FIG. 3, the key manager function 210 includes an analysis function 211, an implementation function 212, and a database 213. The key manager function 210 further includes a communication function 214 including means for receiving network information. Further, the key manager function 210 may receive through the communication function 214 trigger information from any means, including, for example, any network device, attached function, human operator, or administrator, to initiate the analysis and/or replacement encryption key generator 200 operation. The communication function 214 also includes means for the key manager function 210 to exchange messages with one or more network system devices, preferably in a secure manner, including those devices with the replacement encryption key generator 200. The communication function 214 may provide one or more connections to one or more network system devices having the capability to implement replacement encryption key generation, to detect intrusions and report detected intrusions to other devices of the network infrastructure 101, or a combination of both.

[0038] The database 213 of the key manager function 210 preferably includes network information of use in determining whether, where, and/or when to implement replacement encryption key generation. The information may be any type deemed by the network administrator suitable for triggering the generation of encryption key replacement at one or more network system devices including, but not limited to, the number of encrypted messages, path of data flow, endpoint locations, volume of information exchanged, protocol changes, history based information and other defined triggering events in the network. The information may be generated by the administration server 103, some other sort of centralized network infrastructure device, or from a peer, and stored in the database 213. The information is preferably

stored or cached in the database 213 in advance and is not solely supplied in reaction to a triggering condition or event that may be occurring on that particular network system device. The database 213 may further include, for example, means for finding replacement encryption key generators 200, historical information, key-to-implementation device mapping, and the like. The information of storage means 201 may also be stored in database 213 of key manager function 210. Database 213 may contain the information of other key manager functions and/or for network system devices not directly commanded by a particular replacement encryption key generator 200.

[0039] With continuing reference to FIGS. 2 and 3, the analysis function 211 performs the function of evaluating network information, determining whether the information includes one or more triggers requiring initiation of the replacement of one or more encryption keys. The analysis function 201 then notifies the implementation function 212 that a replacement must be performed, and it may notify the implementation function 212 which one or more network system devices should implement the replacement. Alternatively, the implementation function 212 may perform that function. The implementation function 212 then instructs one or more identified replacement encryption key generators 200 to implement an encryption key generation operation and distribution to one or more network system devices, which may include one or more attached functions or network system devices. That instruction is directed to the processor 203 to initiate the replacement. That signaling may be achieved as through communication using unicast, multicast, and/or broadcast communication methods, but not limited thereto.

[0040] As noted, the generated replacement encryption key or keys may be distributed by unicast, multicast, or broadcast distribution including, for example a Layer 2 or Layer 3 multicast protocol distribution. In general, in a forwarding situation, the processor 203 provisions the forwarding engine 202 with the generated replacement encryption keys. Replacement keys may be generated and distributed one at a time or in sets. One or more original encryption keys may be replaced while others are retained. One or more replacement keys may themselves be replaced while others are retained. The generated replacement encryption keys may be associated with signal type, one or more transmission protocols, or one or more sets of protocols. There may be transmit encryption keys and receive encryption keys. The one or more replacement encryption keys may encrypt a portion or all of a particular message or protocol. The replacement encryption key generator 200 may generate replacement encryption keys only or it may generate replacement encryption keys and original encryption keys. The basis for distributing replacement keys may be incremental, random, pseudo-random, or as a product of a mathematical method. Further, the basis for replacing replacement encryption keys may be the same as the basis for distributing the first set of replacement encryption keys. Alternatively, the second and subsequent sets of one or more replacement encryption keys may be distributed for a reason different than the first reason or basis for replacing. In this alternative form, unauthorized data recovery would likely be more difficult as patterning is less likely to occur.

[0041] Referring back to FIG. 1, an attached function such as a service 104a attaches to infrastructure 101 through

connection point 102b (e.g., a jack in a wall). Network infrastructure entry devices 105a-b and central switching device 106 connect to each other using cables and connection points in a similar manner. A connection point is the physical port through which a network client communicates. Referring to FIG. 2, the network system device includes ingress port 207 and an egress port 208. The network system device is configured at ingress port interface 204 to recognize and exchange signals with the attached function and/or other network system devices. The signals pass from the ingress port interface 204 to the forwarding engine 202 for forwarding decisions. Forwarding decisions include, but are not limited to, forwarding through egress port interface 205 received signals to other network infrastructure devices, such as the administration server 103, the application server 107, and the central switching device 106. If authentication is an aspect of the signal exchange or session to be secured by the present invention, an authentication server may also be involved in the initial setup of the session. The forwarding engine 202 may be any type of forwarding function including, but not limited to, a Layer 2 Switch or bridge or a Layer 3 router. The processor 203 communicates with the forwarding engine 202, the database 201, and, via the egress port interface 205, the key manager function 210. One or more of the described interfaces, functions, forwarding engine, and processor may be discrete components, or parts of one or more common components. They may be coupled together as module components in any combination of hardware, firmware, software, microcode or any combination thereof.

[0042] Entry to the network system 100, and the infrastructure 101 primarily, may be initially regulated using authentication systems such as Network Operating Systems (NOSs), Remote Authentication Dial-In User Service (RADIUS), described in IETF RFC 2865 and IEEE 802.1X standard, which provides for port-based network entry control based on a MAC identifier. In the case of NOS and RADIUS, an authentication server provides the mechanism for establishing such authentication. RADIUS may also provide authorization and, optionally, accounting capability related to network usage. In the case of IEEE 802.1X, the network entry devices may be configured with such authentication capability, as described more fully in that standard. IEEE 802.1Q standard provides another means for controlling usage of a network. That standard is directed to the establishment and operation of VLANs. The IEEE 802.1Q standard defines the configuration of network devices to permit packet reception at a configured port entry module. Firewalls also provide a technique for network entry regulation based on their packet analysis functionality previously described. The present invention also contemplates signal exchange protection using the replacement encryption key generator 200 for exchanges that have already been authenticated, or that are not required to be authenticated.

[0043] The following is a list of a few possible devices (but not limited to only those devices) that can contain the replacement encryption key generator 200, the key manager function 210, and/or any one or more of the corresponding functions described herein: network switches, data switches, routers, WAN devices, MAN devices, optical switches, firewalls, gateways including VPN gateways and other transmission devices, computing devices such as network file servers or dedicated usage servers, management stations, Private Exchange Branch (PBX) devices, telecommunica-

tion devices, cellular phones, network connected voice over IP/voice over data systems such as hybrid PBXs and VoIP call managers, network layer address configuration/system configuration servers such as enhanced DHCP servers, enhanced Bootstrap Protocol (bootp) servers, IPv6 address auto-discovery enabled routers, and network based authentication servers providing services such as RADIUS, Extensible Authentication Protocol/IEEE 802.1X or others. It is to be noted that the present invention is applicable to telephone as well data communication network systems.

[0044] One means to provide the network information to the storage means 201 and database 213 is the Simple Network Management Protocol (SNMP). A network administrator provisions the information through the terminus of a network cable associated with the attached function. The forwarding engine 202 or other enforcement function reads the terminus information via the SNMP. In another example, SNMP MIB parameters may be established or used to obtain and configure the storage means 201 and database 213 with the desired information. MIBs may also be employed to populate one or more tables of the network system device operating as generation and/or distribution devices with historical information for storage and/or caching.

[0045] A first embodiment of the security enhancement method of the present invention for a session involving either or both of one or more attached functions and one or more network devices for which authentication may or may not be required, is shown in FIG. 4. The method represented in FIG. 4 includes initial steps generally applicable in the context of existing standards-based protocols. First, a network session is initiated through one or more network system devices (step 301). That initiation may or may not require a step of authentication. The initiation may occur through any well known means, whether in unicast, multicast, or broadcast transmission mode. The session may be initiated in any wired or wireless environment including, for example, in a cable-based physical connection, a radio frequency connection, a VPN connection, an infrared connection, a tunneled endpoint connection, or a shared connection, such as Resilient Packet Ring (RPR), broadband, Passive Optical Network (PON), or Ethernet over First Mile (EFM). First one or more encryption key sets are established at the functions, whether attached functions, network devices, or both for use in securing messages passing to the ingress locations thereof and from the egress locations thereof (step 302). These keys are randomly or pseudo-randomly derived and secured by encryption techniques well known to those skilled in the art including, for example by RC4 by RSA labs, the Data Encryption Standard (DES), triple DES (3DES) or the Advanced Encryption Standard (AES). Optionally, each key set is marked, one as a receive key set and the other as a transmit key set. It is to be understood that for a plurality of attached functions or other network system devices, either of which type may be referred to as an encryption function, each may each receive a unique key set of one or more keys, or a portion or all of those encryption functions may share the same key set. The signal exchange session then proceeds with encrypted signals forwarded by the encryption functions, and forwarded encrypted messages de-encrypted by encryption functions having the applicable encryption key set information (step 303).

[0046] With continuing reference to FIG. 4, the manager function 210 analyzes received network information and

determines whether one or more replacement encryption key sets are to be generated and distributed (step 304). The information that would cause a replacement may be of any type of interest to the network administrator including, for example, signal traffic conditions, protocols, and any others deemed to be of interest. Upon determination that one or more replacement encryption key sets are to be generated and distributed, the key manager function 210 identifies one or more replacement encryption key generators 200 to be activated and one or more network system devices to carry out the replacement (step 305). Instructions are then sent to the identified one or more replacement encryption key generators 200 to generate randomly or pseudo-randomly one or more replacement encryption key sets (step 306). The generated one or more replacement encryption key sets are then distributed to one or more encryption functions (step 307). The distributed replacement encryption key set(s) is/are then employed in encrypting and decrypting signals, including protocols (step 308). The signal exchange and network information analysis are preferably substantially continuous throughout a network session. Optionally, information derived from the network system analysis, the replacement encryption key generation, and the identified of replacement encryption key generators and relevant network system devices may be reported to a reporting function (step 309).

[0047] For any particular attached function, a received encryption key set is preferably stored in a register and accessed as required to encrypt or decrypt a message. In the event a plurality of key sets is already registered, the least recently used or oldest set may be overwritten when a replacement encryption key set is generated and received. In a shared key set environment, the network entry device confirms that all attached functions return a message using the most recent key set, which may include one or more replacement encryption keys. Alternatively, the network entry device may use a fixed number of duplicate key messages, i.e., retries, in the absence of positive acknowledgement from any one or more attached functions that the key messages have been received and processed. Once all relevant attached functions clients are on the correct key set, signal exchanges are continued.

[0048] An important aspect of the present invention is that the key sets, whether randomly generated or not, are changed over the course of any signal exchange session. Current crypto analysis attacks indicate that static keys can often be recovered. For that reason, the present invention includes the replacement of an existing key set with a replacement key set, preferably based on information that ensures the replacement occurs faster than an analysis attack is able to discover the key set in use.

[0049] A second embodiment of the security enhancement method of the present invention for a network session involving an attached function requiring authentication, is shown in FIG. 5. The method represented in FIG. 5 includes initial steps generally applicable in the context of existing standards-based protocols. Specifically, the attached function initiates a network session through a network entry device under a suitable session initiation process, such as the EAP/TLS/S02.1X protocol in a wireless setting, or other protocols in a wired setting (step 401). An authentication server addresses the initiation request by sending an initial session initiation key set to the attached function through the

network entry device (step 402), it being understood that the attached function may instead be a network device, such as in the case of a point-to-point exchange within a network system. The attached function then sends session-encrypted user information to the authentication server for authentication (step 403). Assuming the authentication occurs, the network entry device transmits to the requesting attached function one or more encryption keys and unblocks a port of the device to enable signal exchange pursuant to one or more defined policies (step 404). These keys are pseudo-randomly derived and secured by encryption, using the initial session keys shared with the client. The authentication server or the key manager function 210 sends the session keys and the initial one or more encryption keys to the network entry device as part of the authentication acceptance message. Typically, each key set is marked, one as a client receive key set and the other as a client transmit key set. It is to be understood that a plurality of attached functions or other network system devices associated with a particular network device may each receive a unique key set of one or more keys, or a portion or all of these attached functions may share the same key set. Assuming shared key sets are used, the network entry device enables network system exchanges for a plurality of attached functions using the same initial assigned encryption key set (step 405).

[0050] With continuing reference to FIG. 4, the key manager function 210 analyzes received network information and determines whether one or more replacement encryption key sets are to be generated and distributed (step 406). The information that would cause a replacement may be of any type of interest to the network administrator including, for example, periodic or sporadic time, signal traffic conditions, protocols, and any others deemed to be of interest. Upon determination that one or more replacement encryption key sets are to be generated and distributed, the key manager function 210 identifies one or more replacement encryption key generators 200 to be activated and one or more network system devices to carry out the replacement (step 407). Instructions are then sent to the identified one or more replacement encryption key generators 200 to generate randomly or pseudo-randomly one or more replacement encryption key sets (step 408). The generated one or more replacement encryption key sets are then distributed to one or more attached functions (step 409). The distributed replacement encryption key set(s) is/are then employed in encrypting and decrypting signals, including protocols (step 410). The signal exchange and network information analysis are preferably substantially continuous throughout a network session. Optionally, information derived from the network system analysis, the replacement encryption key generation, and the identified of replacement encryption key generators and relevant network system devices may be reported to a reporting function (step 411).

[0051] For any particular attached function, a received encryption key set is preferably stored in a register and accessed as required to encrypt or decrypt a message. In the event a plurality of key sets is already registered, the least recently used or oldest set may be overwritten when a replacement encryption key set is generated and received. In a shared key set environment, the network entry device confirms that all attached functions return a message using the most recent key set, which may include one or more replacement encryption keys. Alternatively, the network entry device may use a fixed number of duplicate key

messages, i.e., retries, in the absence of positive acknowledgement from any one or more attached functions that the key messages have been received and processed. Once all relevant attached functions clients are on the correct key set, signal exchanges are continued.

[0052] An important aspect of the present invention is that the key sets, whether randomly generated or not, are changed over the course of any signal exchange session. Current crypto analysis attacks indicate that static keys can sometimes be detected. For that reason, the present invention includes the replacement of an existing key set with a replacement key set, preferably based on information that ensures the replacement occurs faster than an analysis attack is able to discover the key set in use.

[0053] It is to be understood that the functions described herein may be implemented in hardware and/or software. For example, particular software, firmware, or microcode functions executing on the network infrastructure devices can provide the implementation function. Alternatively, or in addition, hardware modules, such as programmable arrays, can be used in the devices to provide some or all of those capabilities.

[0054] Other variations of the above examples may be implemented. One example variation is that the illustrated processes may include additional steps. Further, the order of the steps illustrated as part of the process is not limited to the order illustrated in FIGS. 4 and 5, as the steps may be performed in other orders, and one or more steps may be performed in series or in parallel to one or more other steps, or parts thereof.

[0055] The processes, steps thereof and various examples and variations of these processes and steps, individually or in combination, may be implemented as a computer program product tangibly as computer-readable signals on a computer-readable medium, for example, a non-volatile recording medium, an integrated circuit memory element, or a combination thereof. Such computer program product may include computer-readable signals tangibly embodied on the computer-readable medium, where such signals define instructions, for example, as part of one or more programs that, as a result of being executed by a computer, instruct the computer to perform one or more processes or acts described herein, and/or various examples, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBOL, and the like, or any of a variety of combinations thereof. The computer-readable medium on which such instructions are stored may reside on one or more of the components of system 100 described above and may be distributed across one or more such components.

[0056] A number of examples to help illustrate the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the claims appended hereto.

What is claimed is:

1. A method for enhancing the security of a network having one or more network devices including one or more

network infrastructure devices capable of exchanging messages, the method comprising the steps of:

- a. generating a plurality of encryption keys;
 - b. encrypting some or all of the messages exchanged between two or more of the network infrastructure devices, or exchanged within one or more of the network infrastructure devices, with one or more of the plurality of encryption keys; and
 - c. in the course of the message exchanges, replacing one or more of the one or more encryption keys with one or more replacement encryption keys.
2. The method of claim 1 wherein at least one of the plurality of encryption keys is designated for transmission selected from the group consisting of multicast transmissions, for broadcast transmissions, and unicast transmissions.
3. The method of claim 1 wherein some or all of the plurality of encryption keys are replaced as a function of the number of encrypted messages, randomly, or the amount of information exchanged during the message exchanges.
4. The method of claim 1 wherein at least one of the one or more network infrastructure devices is selected from the group consisting of wireless access points, routers, VPN gateways, and switches.
5. The method of claim 1 wherein the plurality of encryption keys are randomly generated.
6. The method of claim 1 wherein the one or more replacement encryption keys are randomly generated.
7. The method of claim 1 wherein the encryption keys are protocol encryption keys.
8. The method of claim 1 further comprising the step of replacing one or more of the one or more replacement encryption keys.
9. The method of claim 8 wherein the step of replacing one or more of the one or more replacement keys is performed on a basis that is different from the basis for first replacing the one or more plurality of encryption keys, wherein the basis for replacement is selected from the group consisting of incremental replacement, random replacement, pseudo-random replacement, and mathematical algorithm replacement.
10. The method of claim 1 wherein the messages are exchanged across a transmission medium selected from the group consisting of wired, radio frequency, WAN, VPN, infrared, RPR ring, PON, and Ethernet over First Mile.
11. A method for enhancing the security of a network including one or more network devices capable of providing access to the network for one or more attached functions, the method comprising the steps of:
- a. generating a plurality of encryption keys for use in encrypting message exchanges between the one or more attached functions and the network;
 - b. using the plurality of encryption keys in the message exchanges between the one or more network access devices and the one or more attached functions;
 - c. generating one or more replacement encryption keys; and
 - d. during the session, replacing one or more of the plurality of encryption keys with the one or more replacement encryption keys at non-regular intervals.

12. The method of claim 11 wherein the plurality of encryption keys and the one or more replacement encryption keys are randomly generated.

13. The method of claim 11 wherein at least one of the one or more network access devices generates and transmits the plurality of encryption keys and the one or more replacement encryption keys.

14. The method of claim 11 wherein at least two of the plurality of encryption keys is unique to each attached function.

15. The method of claim 11 wherein some or all of the plurality of encryption keys are replaced as a function of the number of encrypted messages, randomly, or as a function of the amount of information exchanged.

16. The method of claim 11 further comprising the step of replacing one or more of the one or more replacement encryption keys.

17. The method of claim 16 wherein the step of replacing one or more of the one or more replacement keys is performed on a basis that is different from the basis for first replacing the one or more plurality of encryption keys, wherein the basis for replacement is selected from the group consisting of incremental replacement, random replacement, pseudo-random replacement, and mathematical algorithm replacement.

18. The method of claim 11 wherein at least one of the plurality of encryption keys is designated for multicast transmissions or broadcast transmissions.

19. The method of claim 11 wherein at least one of the plurality of encryption keys is associated with a transmission protocol.

20. The method of claim 11 wherein at least one of the plurality of encryption keys is associated with a set of transmission protocols.

21. The method of claim 11 wherein at least one of the plurality of encryption keys is a retained encryption key that is not replaced when others of the plurality of encryption keys are replaced.

22. A method for enhancing the security of a network including one or more network devices capable of providing access to the network, the method comprising the steps of:

a. generating a plurality of encryption keys for use in encrypting messages between the one or more network access devices and one or more attached functions;

b. encrypting some or all of the messages with one or more of the plurality of encryption keys; and

c. in the course of exchanging messages with the one or more attached functions, without authenticating, transmitting to the one or more attached functions one or more replacement encryption keys to replace one or more of the one or more encryption keys.

23. The method of claim 22 wherein the plurality of encryption keys and the one or more replacement encryption keys are randomly generated.

24. The method of claim 22 wherein at least one of the one or more network devices generates the one or more encryption keys and the one or more replacement encryption keys.

25. The method of claim 22 wherein at least one of the attached functions is selected from the group consisting of an internet interface function, a VPN interface function, and a wireless interface function.

26. The method of claim 22 wherein some or all of the plurality of encryption keys are replaced as a function of the number of encrypted messages, randomly, or as a function of the amount of information exchanged during the message exchanges.

27. The method of claim 22 further comprising the step of replacing one or more of the one or more replacement encryption keys.

28. The method of claim 27 wherein the step of replacing one or more of the one or more replacement keys is performed on a basis that is different from the basis for first replacing the one or more plurality of encryption keys, wherein the basis for replacement is selected from the group consisting of incremental replacement, random replacement, pseudo-random replacement, and mathematical algorithm replacement.

* * * * *

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200810085794.0

[51] Int. Cl.

H04L 9/00 (2006.01)

H04L 12/58 (2006.01)

H04L 12/18 (2006.01)

[43] 公开日 2009 年 9 月 30 日

[11] 公开号 CN 101547086A

[22] 申请日 2008.3.24

[21] 申请号 200810085794.0

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 阳振庭

[74] 专利代理机构 北京挺立专利事务所

代理人 叶树明

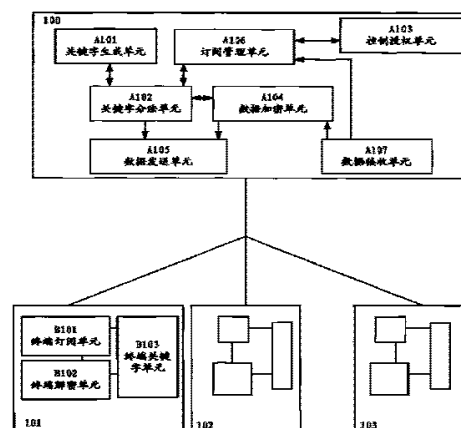
权利要求书 4 页 说明书 15 页 附图 6 页

[54] 发明名称

一种宽带接入网络组播控制方法、系统及装置

[57] 摘要

本发明实施例公开了一种宽带接入网络组播控制系统、方法及设备，该系统包括：接入控制子系统，用于生成组播加密关键字，将所述组播加密关键字发送给用户子系统，并在接收到用户子系统发送的订阅请求后，利用所述组播加密关键字对发往用户子系统的组播帧进行加密，将所述加密过的组播帧发送到所述用户子系统；用户子系统，用于向所述接入控制子系统发送订阅请求来请求组播帧，根据接收的接入控制子系统发送的组播加密关键字解密接收到的所述接入控制子系统加密过的组播帧。本发明在广播式（共享介质）接入应用中，授权用户才能使用组播业务数据，防止非法用户使用组播业务，增强了组播权限控制的安全性。



1、一种宽带接入网络组播控制系统，其特征在于，包括：

接入控制子系统，用于生成组播加密关键字，将所述组播加密关键字发送给用户子系统，并在接收到用户子系统发送的订阅请求后，利用所述组播加密关键字对发往用户子系统的组播帧进行加密，将所述加密过的组播帧发送到所述用户子系统；

用户子系统，用于向所述接入控制子系统发送订阅请求来请求组播帧，根据接收的接入控制子系统发送的组播加密关键字解密接收到的所述接入控制子系统加密过的组播帧。

2、如权利要求1所述宽带接入网络组播控制系统，其特征在于，所述接入控制子系统包括：

关键字生成单元，用于生成组播加密关键字集合，所述组播加密关键字集合包括至少一个组播加密关键字及对应的组播流标识；

关键字分发单元，用于向用户子系统发送所述关键字生成单元生成的组播加密关键字；

数据接收单元，用于接收来自组播源设备的组播帧以及来自用户子系统的组播订阅请求，并将所述组播帧发送到数据加密单元；

数据加密单元，用于从组播订阅请求中解析出的组播流标识，根据所述组播流标识从所述关键字生成单元的组播加密关键字集合中获取组播加密关键字，并利用所述关键字生成单元生成的组播加密关键字及对应的加密算法对发往用户子系统的组播帧进行加密，并将加密过的组播帧发送到数据发送单元；

数据发送单元，用于确定所述数据接收单元接收到用户子系统发送的订阅请求后，根据组播转发表向用户子系统发送所述数据加密单元加密过的组播帧。

3、如权利要求2所述宽带接入网络组播控制系统，其特征在于，所述接入控制子系统还包括：

订阅管理单元，用于接收所述数据接收单元的用户子系统的组播订阅请

求后建立所述组播转发表，接收到用户子系统的撤离请求时，删除所述组播转发表。

4、如权利要求2所述宽带接入网络组播控制系统，其特征在于，所述关键字分发单元还用于：

检测到关键字刷新或切换事件，通知所述关键字生成单元生成一个或多个组播加密关键字，将新的组播加密关键字通知用户子系统。

5、如权利要求4所述宽带接入网络组播控制系统，其特征在于，
所述刷新或切换事件包括定时触发、或接收到所述接入控制子系统发送的订阅撤离请求。

6、如权利要求2所述宽带接入网络组播控制系统，其特征在于，所述接入控制子系统还包括：

控制授权单元，用于根据组播订阅请求中的订阅参数和用户标识信息对发送所述订阅请求的用户子系统进行鉴权，确定所述用户子系统访问组播流的权限。

7、如权利要求1至4中任一项所述宽带接入网络组播控制系统，其特征在于，所述接入控制子系统为光线路终端OLT，所述用户子系统为光网络单元ONU或主机；或

所述接入控制子系统为IP边缘设备或数字用户线接入复用器DSLAM；所述用户子系统为RG或主机。

8、一种宽带接入网络组播控制方法，其特征在于，包括以下步骤：

生成并分发组播加密关键字集合，所述组播加密关键字集合包括至少一个组播加密关键字及对应的组播流标识；

接收到订阅请求后，利用所述组播加密关键字对组播帧进行加密；

发送所述加密过的组播帧，所述加密过的组播帧能用所述组播加密关键字进行解密。

9、如权利要求8所述宽带接入网络组播控制方法，其特征在于，所述利用所述组播加密关键字对组播帧进行加密具体包括：

从组播订阅请求中解析出组播流标识;

根据所述组播流标识从所述组播加密关键字集合中获取组播加密关键字;

利用所述组播加密关键字及对应的加密算法对组播帧进行加密。

10、如权利要求8所述宽带接入网络组播控制方法,其特征在于,所述生成并分发组播加密关键字之后还包括:

检测到关键字刷新或切换事件,更新所述组播加密关键字。

11、如权利要求10所述宽带接入网络组播控制方法,其特征在于,所述刷新或切换事件包括定时触发、或接收到订阅撤离请求。

12、一种接入控制装置,其特征在于,包括:

关键字生成单元,用于生成组播加密关键字集合,所述组播加密关键字集合包括至少一个组播加密关键字及对应的组播流标识;

关键字分发单元,用于向用户子系统发送所述关键字生成单元生成的组播加密关键字;

数据接收单元,用于接收来自组播源设备的组播帧以及来自用户子系统的组播订阅请求,并将所述组播帧发送到数据加密单元;

数据加密单元,用于从组播订阅请求中解析出的组播流标识,根据所述组播流标识从所述关键字生成单元的组播加密关键字集合中获取组播加密关键字,并利用所述关键字生成单元生成的组播加密关键字及对应的加密算法对发往用户子系统的组播帧进行加密,并将加密过的组播帧发送到数据发送单元;

数据发送单元,用于确定所述数据接收单元接收到用户子系统发送的订阅请求后,根据组播转发表向用户子系统发送所述数据加密单元加密过的组播帧。

13、如权利要求12所述接入控制装置,其特征在于,所述接入控制子系统还包括:

订阅管理单元,用于接收所述数据接收单元的用户子系统的组播订阅请

求后建立所述组播转发表，接收到撤离请求时，删除所述组播转发表。

一种宽带接入网络组播控制方法、系统及装置

技术领域

本发明涉及通信技术领域，尤其涉及一种宽带接入网络组播控制方法、系统及装置。

背景技术

随着网络逐步宽带化，新业务不断涌现，尤其 IPTV（因特网电视）类业务得到大量应用。由于 IPTV 业务一般是组播（多播）应用模式，即同一份数据多人同时共享，如不同用户观看同一个电视频道/节目，这给网络的权限管理带来不小困难。

在 DSL（Digital Subscriber Line，数字用户线）用户中，一般在网络边缘的组播鉴权装置中进行组播权限控制，组播鉴权装置包括接入节点（Access Node，AN），一般在组播鉴权装置中设置用户的组播权限控制表，例如：组播访问控制表（Access Control List，ACL）。组播鉴权装置通过组播权限控制表控制用户对组播频道的访问，由于 DSL 一般是点到点接入（即：连接的路径是独占的），通过组播权限控制表能够有效控制用户对组播频道的访问，但是对于广播式（共享介质）接入，组播流（连续传递的多个组播帧称之为组播流）是广播（多播）发送的，即一个用户请求了一份组播流，处于这个广播域中的用户都能收到该份组播流。

广播式（共享介质）接入主要包括 PON（Passive Optical Network，无源光网络）、WIMAX（Worldwide Interoperability for Microwave Access，全球微波互联接入）等。例如：一个 PON 接口下的一个用户观看一个节目频道，这个 PON 接口内的所有用户都能够收到这个节目的组播流，即这个 PON 内的所有用户都能够观看这个节目，由于组播的点对多点传递特性，组播成员共享组播流，所以不能采用点对点的加密。

现有技术中通过广播电视系统的 CA（条件接收）系统进行组播权限控制，

主要应用在广播电视领域，如数字电视领域，广播电视系统的CA系统主要是在头端系统进行应用层加密，然后通过机顶盒（STB）进行条件接收。

现有技术中，在头端进行集中控制授权，系统实现复杂，容易引起性能瓶颈；一般要求内嵌智能卡的机顶盒，不利于运营商之间媒体内容共享；且广播电视系统的CA系统并不适合在宽带网络应用。

发明内容

本发明实施例提供了一种宽带接入网络组播控制方法、系统及装置，合法的组播成员用户才能使用组播业务数据，防止非法用户使用组播业务。

本发明实施例提供了一种宽带接入网络组播控制系统，包括：

接入控制子系统，用于生成组播加密关键字，将所述组播加密关键字发送给用户子系统，并在接收到用户子系统发送的订阅请求后，利用所述组播加密关键字对发往用户子系统的组播帧进行加密，将所述加密过的组播帧发送到所述用户子系统；

用户子系统，用于向所述接入控制子系统发送订阅请求来请求组播帧，根据接收的接入控制子系统发送的组播加密关键字解密接收到的所述接入控制子系统加密过的组播帧。

本发明实施例还提供了一种宽带接入网络组播控制方法，包括以下步骤：

生成并分发组播加密关键字集合，所述组播加密关键字集合包括至少一个组播加密关键字及对应的组播流标识；

接收到订阅请求后，利用所述组播加密关键字对组播帧进行加密；

发送所述加密过的组播帧，所述加密过的组播帧能用所述组播加密关键字进行解密。

本发明实施例一种接入控制装置，包括：

关键字生成单元，用于生成组播加密关键字集合，所述组播加密关键字集合包括至少一个组播加密关键字及对应的组播流标识；

关键字分发单元，用于向用户子系统发送所述关键字生成单元生成的组播加密关键字；

数据接收单元，用于接收来自组播源设备的组播帧以及来自用户子系统的组播订阅请求，并将所述组播帧发送到数据加密单元；

数据加密单元，用于从组播订阅请求中解析出的组播流标识，根据所述组播流标识从所述关键字生成单元的组播加密关键字集合中获取组播加密关键字，并利用所述关键字生成单元生成的组播加密关键字及对应的加密算法对发往用户子系统的组播帧进行加密，并将加密过的组播帧发送到数据发送单元；

数据发送单元，用于确定所述数据接收单元接收到用户子系统发送的订阅请求后，根据组播转发表向用户子系统发送所述数据加密单元加密过的组播帧。

本发明的实施例中，在广播式（共享介质）接入应用中，授权用户才能使用组播业务数据，防止非法用户使用业务。加强了在共享介质接入的组播安全控制，杜绝了未授权或恶意访问，保护了运营商的投资。

附图说明

- 图 1 是本发明实施例中宽带接入网络组播控制系统；
- 图 2 是本发明实施例中在 PON 系统中的应用示意图；
- 图 3 是本发明实施例中组播业务控制流程图；
- 图 4 是本发明实施例中 PON 系统的关键字刷新或切换流程图；
- 图 5 是本发明实施例中常用共享介质系统的应用流程图；
- 图 6 是本发明实施例中加密前的明文组播帧示意图；
- 图 7 是本发明实施例中加密后的组播帧示意图；
- 图 8 是本发明实施例中吉比特无源光网络帧结构；
- 图 9 是本发明实施例中吉比特无源光网络关键字消息结构；
- 图 10 是本发明实施例中以太网无源光网络关键字消息结构。

具体实施方式

本发明实施例中提供了一种宽带接入网络组播控制系统，可应用于 PON

或常用共享介质等系统中，如图 1 所示，包括：接入控制子系统 100 和用户子系统 101、102、103。其中，

接入控制子系统 100 包括：关键字生成单元（Key Generator Unit, KGU）A101、关键字分发单元（Key Distribution Unit, KDU）A102、控制授权单元（Control Authorization Unit, CAU）A103、数据加密单元（Data Encryption Unit, DEU）A104、数据发送单元（Data Sending Unit, DSU）A105、订阅管理单元（Subscription Control Unit, SCU）A106、数据接收单元（Data Receiving Unit, DRU）A107；

用户子系统分别包括：终端订阅单元（Client Subscription Unit, CSU）B101、终端解密单元（Client Decryption Unit, CDU）B102、终端关键字单元（Client Key Unit, CKU）B103。

接入控制子系统 100 可以实现在一台设备中，所述的设备包括：DSLAM（Digital Subscriber Line Access Multiplexer，数字用户线接入复接器）、NAS（Network Access Server，网络访问服务器）、边缘路由器、基站等，也可以是多台设备组成（不同的单元分布在不同的设备上）；CSU B101 与 CDU B102 和 CKU B103 可以分布在不同用户终端中，CDU B102 和 CKU B103 一般集成在一个设备中。

其中，KGU A101，用于生成组播加密关键字集合（Multicast Encryption Key, MEK），该集合中包括一个或多个组播加密关键字，这些组播加密关键字与组播流标识相对应，MEK 用于对组播帧进行加密或解密。组播帧的加密和解密关键字一般使用对称关键字，关键字（或称之为密钥）长度和类型根据具体实现决定，DEU A104 用 MEK 对组播帧进行加密，用户子系统的 CDU B102 用 MEK 对加密后的组播帧进行解密，KGU A101 一般通过伪随机函数（pseudo-random function, PRF）产生一个随机数，再根据此随机数生成 MEK。

KDU A102，用于管理 MEK，包括维护 MEK 的状态、向用户子系统分发 MEK、通知用户子系统刷新或切换 MEK 等，例如：KDU A102 向用户子系统的 CKU B103 分发 MEK 或 KDU A102 通知用户子系统的 CKU B103 进行 MEK 切换。分发 MEK 以及刷新切换 MEK 通知消息的实现协议可以根据具体实现

决定，可以包括：OMCI、IGMP、MLD、CAPWAP、MPCP（Multi-Point Control Protocol，多点控制协议）、OAM（Operations Administration and Maintenance，操作维护管理）等，MEK 可以使用接入控制子系统和用户子系统事先协商的点对点关键字加密后分发，所述的事先协商的点对点关键字包括：预先共享（pre-shared）的点对点关键字、用户子系统通知给接入控制子系统的公用点对点关键字（public-key）等。在组播（或称多播）应用中，一个或者多个组播流共享一个 MEK，所有合法的用户子系统（即组播成员）使用 MEK 解密组播帧。KDU A102 管理维护的 MEK 如表 1 所示：

表 1 MEK 状态表

组播流标识	MEK 值	MEK 切换周期
225.1.100.1	MEK1	5 分钟
226.1.100.1	MEK2	10 分钟
227.100.1.1/24		
0x01-00-5E-00-01-10	MEK3	6 分钟
...		

其中 227.100.1.0/24 表示范围，表示 227.100.1.0 到 227.100.1.255 的所有组播流标识。

CAU A103，用于对用户子系统的订阅请求进行鉴权，例如：通过组播权限控制表对用的组播请求进行控制，组播权限控制表 2 所示：

表 2 组播权限控制表

用户标识	组播组	权限
用户 A	225.1.100.1	允许
	224.100.1.1/24	拒绝
	239.1.1.1， 10.1.1.1	允许
	...	
用户 B	FF05:0:0:0:0:0:2	拒绝
...		

组播权限控制表一般预先配置，通过组播权限控制表可以确定一个用户访问

一个组播流或多个组播流的权限。

DEU A104, 用于加密组播帧, 所述的组播帧指发往用户子系统的组播帧, DEU A104 采用的加密方法 (算法) 可以根据具体的实现而定, 如使用 IPSec 加密、IEEE (Institute of Electrical and Electronics Engineers, 电气和电子工程师学会) 802.1ae 的 MACSec 加密、PON 层加密、无线空口加密、SRTP (Secure Real-time Transport Protocol, 安全实时流传输协议) 加密等。

DSU A105, 用于发送数据, 包括 DEU A104 加密后的组播帧、MEK 分发或切换消息等。

SCU A106, 用于处理组播订阅请求, 如处理用户子系统的 CSU B101 发送的 IGMP 或 MLD 报告 (Report) 消息, SCU A106 具体可以是一个 IGMP/MLD 探测 (snooping) 或代理 (Proxy)。

DRU A107, 用于接收数据, 包括接收来自组播源设备的组播帧、来自用户子系统的组播订阅请求等。

本发明实施例在 PON 系统中的应用如图 2 所示: PON 由安装于中心控制站的光线路终端 (Optical Line Terminals, OLT)、光配线网 (Optical Distribution Network, ODN) 和安装在用户场所的光网络单元 (Optical Network Unit, ONU) 三部分组成。在下行方向采用广播的方式传输数据帧, 上行方向采用复用方式完成多个 ONU 的接入。接入控制子系统 100 为 OLT 设备, 用户子系统 101、102、103 为 ONU (ONT) 设备和/或主机。CDU B102 和 CKU B103 位于 ONT 中, CSU B101 可以实现在 ONT 或主机中。KGU A101、KDU A102、CAU A103、DEU A104、DSU A105、SCU A106、DRU A107 实现在 OLT 中。下面描述接入控制子系统 100 和用户子系统的处理。

接入控制子系统 100 的处理包括控制面处理和数据面处理, 其中数据面处理包括:

接入控制子系统 100 接收到组播源发送的组播流 (Multicast Flow, MC Flow), 将组播数据流进行加密, 然后将加密后的组播流转发至用户子系统, 需要说明的是, 对于一个 PON 接口, 接入控制子系统 100 发送一份或者多份组播流, 由于 PON 是广播发送的, 因此所有的用户子系统都可以收到接入控制

子系统发送的组播流。具体实现可以是：DRU A107接收到组播源发送的组播流中的组播帧后，DRU A107将组播帧交给DEU A104进行加密，DEU A104根据组播帧的组播流标识获取组播帧加密的MEK，然后按照对应的加密算法和MEK对组播帧进行加密，DEU A104将加密后的组播帧交给DSU A105，DSU A105再根据组播转发表将组播帧转发出去，组播转发表一般由SCU A106建立和删除，组播转发表包括流标识以及转发出口（例如：端口），所述的流标识可以从组播帧的IP或以太网首部的目的（即组播）地址字段中获取。

接入控制子系统100的控制面处理包括：

接入控制子系统100接收到组播订阅请求，解析所述的订阅请求获取组播流标识等订阅参数以及用户标识信息，然后根据所述的组播流标识获取该组播流标识对应的MEK，然后将该MEK分发到发起该订阅请求的用户子系统，同时建立组播转发表以及将用户子系统作为组播成员并记录其状态。优选的，接入控制子系统100接收到订阅请求后还包括对该订阅请求进行鉴权处理，如果鉴权失败，则不分发MEK。具体实现可以是：DRU A107接收到订阅请求消息后，DRU A107将该消息交给SCU A106处理，SCU A106解析该消息，获取订阅参数和用户标识信息，CAU A103根据SCU A106提供的订阅参数和用户标识信息进行鉴权处理，SCU A106通知KDU A102分发MEK。KDU A102首先检查组播流标识的MEK是否已经存在，如果不存在则请求KGU A101生成一个新的MEK。

接入控制子系统100接收到组播订阅撤离，接入控制子系统100可以刷新或切换该订阅撤离包括的组播流标识对应的MEK。接入控制子系统100可以支持周期性的刷新MEK。刷新MEK具体可以是KDU A102请求KGU A101生成一个新的MEK，然后将MEK保存起来，同时将MEK通过MEK分发协议消息发送到用户子系统。

用户子系统的处理包括控制面处理和数据面处理，其中数据面处理包括：

用户子系统接收到接入控制子系统100发送的加密后的组播帧，根据所述的组播帧的组播流标识获取对应的MEK，然后使用MEK解密所述加密后的组播帧，具体实现可以是用户子系统的CDU B102根据组播流标识，从CKU B103

中获取MEK。

用户子系统的控制面处理包括:

用户子系统接收到接入控制子系统 100 发送的 MEK 分发消息或切换消息, CKU B103 根据该消息保存 MEK 或进行 MEK 切换。用户子系统可以支持根据组播流中的组播帧的切换标识进行 MEK 切换, 也可以根据时间定时切换。

用户子系统向接入控制子系统 100 发送订阅请求或撤离消息, 通知接入控制子系统 100 进行订阅或撤离处理。

本发明实施例在 PON 系统中的处理如图 3 所示, 接入控制子系统 100 为 OLT 设备, 用户子系统为 ONU (ONT) 设备和/或主机, 主要包括以下步骤:

S301, 用户子系统开始组播订阅请求, 例如: 主机发送加入 (Join) 请求, 具体如: 主机的 CSU B101 发送 IGMP 或 MLD 报告 (REPORT) 消息, 订阅请求可以包含订阅参数、用户标识信息等, 用户标识信息具体包括主机的 IP 地址、MAC 地址、终端标识等。订阅参数包括组播流标识, 例如: 组播组地址。

S302, 接入控制子系统进行订阅请求处理。OLT 的 DRU A107 接收到加入请求消息, 交由 SCU A106 处理订阅请求, 如解析 IGMP 或 MLD 报告消息, 获取订阅参数和用户标识信息, 用户标识信息还可以包括 OLT 接收到所述的加入请求消息的 OLT 设备端口, CSU B101 通知 CAU A103 对用户子系统的订阅请求进行鉴权, 如果鉴权成功, 则通知 KDU A102 给用户终端分发 MEK, 同时 SCU A106 配置组播转发表, 将用户子系统的用户标识作为组播成员增加到组播成员状态记录中。CAU A103 的鉴权具体包括: CAU A103 根据用户的订阅参数和用户标识信息, 查验用户的组播权限控制表, 如组播 ACL 表, 用户订阅的组播流标识对应的权限为允许, 则鉴权成功。

S303, OLT 分发 MEK。OLT 的 KDU A102 根据用户标识信息获取发送该订阅请求的用户子系统对应的 CKU B103 所在设备的标识, 如 ONU 标识 (ID) 或 GEM PORT 信息或 ONU 的 MAC 地址或 LLID (逻辑链路标识), OLT 的

KDU A102 将 MEK 通过 MEK 分发协议消息发送到用户子系统。OLT 可以通过点对点关键字对 MEK 或 MEK 分发协议消息进行加密。MEK 分发协议消息可以包括组播流标识、加密算法，进一步可以包括时间戳 (timestamp)。例如: OLT 采取 OMCI 分发 MEK, KDU A102 将 MEK 作为 OMCI 的 ME (Manage Entity, 管理实体) 封装到 OMCI 消息中, 发送 OMCI 设置 (Set) 消息 (OMCI 消息中的消息类型编码为 8) 到指定的 ONU, 具体可以是在 OMCI 定义一个多播关键字 ME (Multicast key info), 多播关键字 ME 对应一个类型编号 (class value, 对应于 Message Identifier 前两位), 多播关键字 ME 包括组播流标识、MEK 值、加密类型。组播流标识对应组播帧的标识, 可以是一个组播地址或一个时间戳或端口标识 (PORTID)。

S304, 用户子系统受理 MEK。ONU 接收到 MEK 分发协议消息, 解析该消息获取 MEK, 然后存储 MEK 以及对应的信息, 例如: 组播流标识、加密类型, 时间戳等。

S305, 接入控制子系统加密组播流。OLT 的 DEU A104 加密 DRU A107 接收到的组播帧, DRU A107 接收上行设备 (例如: IP 边缘设备) 发送的组播帧, 获取的组播帧的组播流标识, 根据组播流标识获取 MEK, DEU A104 加密算法 (类型) 可以协定, 本实施例中, DEU A104 实现 PON 的 AES 等算法加密 ATM 或 GEM 帧或以太网帧的数据载荷 (payload) 部分。

S306, 接入控制子系统转发组播帧。OLT 的 DSU A105 将加密后的组播帧向用户子系统发送出去, DSU A105 根据 SCU A106 配置的组播转发表转发加密后的组播帧, 即 DSU A105 只将组播帧发往已经存在用户子系统 (组播成员) 的 PON 端口。

S307, 用户子系统解密组播帧。ONU 的 CDU B102 根据 CKU B103 的 MEK 解密接收到的组播帧, 然后将解密后的组播帧发往主机。

本发明实施例二中, PON 系统的 MEK 刷新或切换应用图, 接入控制子系统 100 为 OLT 设备, 用户子系统 101、102、103 为 ONU (ONT 设备和/或主机, OLT 设备使用 MEK 分发或切换协议消息通知 ONU/ONT。流程如图 4 所示, 主

要包括以下步骤:

S401, 接入控制子系统检测 MEK 刷新或切换事件, 触发 MEK 刷新或切换。OLT 的 KDU A102 检测 MEK 切换事件, MEK 刷新或切换事件包括定时 (period) 触发刷新或切换事件、接入控制子系统 100 接收到订阅撤离 (例如: 组播成员离开) 触发 (如 SCU A106 收到用户的 IGMP 离开消息)。

S402, 接入控制子系统进行 MEK 刷新或切换。OLT 的 KDU A102 检测到 MEK 刷新或切换事件, 开始 MEK 刷新或切换、OLT 的 KDU A102 一次可以刷新或切换一个或多个组播流的 MEK, OLT 的 KDU A102 通知 KGU A101 生成一个或多个 MEK, 然后 KDU A102 获取 KGU A101 生成的 MEK, OLT 的 KDU A102 向 SCU A106 查询待刷新或切换 MEK 的组播成员状态记录, KDU A102 将新的 MEK 以及组播流标识或切换标记封装到 MEK 分发或切换协议消息, 然后使用 MEK 分发或切换协议消息向组播成员记录中的用户子系统成员通知新的 MEK 或切换 MEK。所述的切换标记包括时间或帧标记, 用于指示用户子系统的 CDU B102 启用新的 MEK 进行解密组播帧, 例如: GPON 系统中的超帧 (Ident) 中的复帧计数器值。

S403, 用户子系统进行 MEK 切换或刷新处理。ONU 接收到 MEK 分发或切换协议消息 (例如: OAM 消息), 解析该消息, 获取新的 MEK 或切换 MEK 的切换标记, 然后存储新的 MEK 或切换 MEK 的切换标记。

S404, 接入控制子系统使用新的 MEK 加密组播帧。OLT 的 DEU A104 切换到新的 MEK 加密组播帧, 例如: 在约定时间使用新的 MEK 加密 DRU A107 接收到的组播帧。

S405, 接入控制子系统转发加密后的组播帧。OLT 的 DSU A105 将加密后的组播帧向用户子系统发送出去。

S406, 用户子系统使用新的 MEK 解密组播帧。例如: ONU 的 CDU B102 在约定时间使用 CKU B103 中新的 MEK 解密接收到的组播帧, 然后将解密后的组播帧发往主机。

本发明实施例三, 常用共享介质系统的应用图, 接入控制子系统100为接

入设备，如DSLAM或IP边缘设备，用户子系统101、102、103为RG和/或主机，DSLAM或IP边缘设备以及RG支持IPSec加密或MACSec加密或SRTP，组播流实现IPSec加密或MACSec加密或SRTP加密，IPSec加密时可以只需要使用ESP，MEK分发或切换消息的实现协议不限，例如：SNMP协议或CAPWAP（Control And Provisioning of Wireless Access Points，无线访问点控制和部署协议）或TR-069或IKE。流程如图5所示，包括以下步骤：

S501，IP边缘设备或DSLAM的DSU A105收到订阅请求，开始处理订阅请求（例如：通知KDU A102给用户终端分发MEK，同时SCU A106配置组播转发表，记录组播成员状态）。所述的订阅请求可能来源于应用服务器（例如：AAA服务器或策略控制器或网管服务器）中转的，IP边缘设备或DSLAM的DSU A105收到的订阅请求由于经过应用服务器中转的，所以可以不需要继续对订阅请求进行鉴权，订阅请求可以包括发放的组播流标识和用户标识信息，组播流标识包括组播组地址，用户标识信息包括端口、终端或主机的地址等。此时IP边缘设备或DSLAM可以没有CAU A103和不具备鉴权功能。

S502，IP边缘设备或DSLAM的KDU A102分发MEK，即将MEK通知给用户子系统，IP边缘设备或DSLAM的KDU A102将MEK或组播流标识等信息封装到MEK分发消息中，发送该消息到用户子系统。组播流标识包括组播组IP地址、组播MAC地址、SPI等，KDU A102分发MEK一般采取安全通道，即KDU A102使用点对点关键字加密MEK或MEK分发消息后才发送出去。

S503，受理MEK。RG接收到IP边缘设备或DSLAM的KDU A102的MEK分发消息，获取MEK交由CKU B103处理，例如：保存MEK信息。

S504，IP边缘设备或DSLAM的DEU A104加密组播组帧，例如：IP边缘设备或DSLAM的DEU A104可以使用IPSec的ESP加密，也可以使用MACSec加密，优选的使用IPSec的ESP加密，加密组播帧的MEK根据组播流标识从KDU A102获取。

S505，IP边缘设备或DSLAM的DSU A105将加密后的组播帧向用户子系统发送出去。

S506, RG 的 CDU B102 根据 CKU B103 的 MEK 解密接收到的组播帧,然后将解密后的组播数据帧发往主机。

S507, IP 边缘设备或 DSLAM 的 KDU A102 检测 MEK 刷新或切换事件, MEK 刷新或切换事件包括定时触发切换事件、订阅撤离触发、管理操作指令触发。需要说明的是,如果是订阅撤离触发,IP 边缘设备或 DSLAM 会将用户子系统作为组播成员从组播成员状态记录中删除。

S508, IP 边缘设备或 DSLAM 的 KDU A102 检测到 MEK 刷新或切换事件,开始 MEK 刷新或切换、发送 MEK 刷新或切换消息,通知该组播组的所有用户子系统新的 MEK 或切换标记, A102KDU 需要根据 DSU A105 保存的该组播成员状态记录逐一通知,一般的,一个组播组的成员对应一个用户子系统。

S509, RG 接收到 IP 边缘设备或 DSLAM 的 KDU A102 的 MEK 刷新或切换消息,获取新的 MEK 或切换标记交由 CKU B103 处理(例如:保存)。

S510, 启用新的 MEK 加密组播帧。例如: IP 边缘设备或 DSLAM 的 DEU A104 在约定时间使用新的 MEK 加密 DRU A107 接收到的组播帧, DEU A104 可以在加密的组播帧中设置 MEK 切换标记。

S511, IP 边缘设备或 DSLAM 的 DSU A105 将加密后的组播帧向用户子系统发送出去。

S512, 用户子系统使用新的 MEK 解密组播帧。例如: RG 的 CDU B102 在约定时间或根据加密组播帧的切换标记使用 B103CKU 中新的 MEK 解密接收到的组播帧,然后将解密后的组播帧发往主机。

本发明实施例四详细描述采用 IPsec ESP 加密和解密组播帧的方法,加密组播帧指将明文组播帧经过数据计算后转换成密文组播帧,解密组播帧指将密文组播帧经过数据计算后还原成明文组播帧。在本实施例中,接入控制子系统接收到的组播源发送的组播帧为明文组播帧,组播帧一般包括 IP 载荷 603 和 IP 首部 602,如图 6 所示,IP 载荷 603 包括的是组播业务数据 604,IP 首部 602 包括目的 IP (Destination Address) 602A 和源 IP (Source Address) 602B,目的 IP 602A 一般是一个组播组地址,源 IP (Source Address) 602B

是发送组播帧的源设备的 IP 地址。IP 首部 602 之前还可以包括链路层首部 601，如以太网首部。

IPSec 加密组播帧可以使用隧道模式和透明模式，优选使用透明模式，如图 7 所示，使用 IPSec 透明模式加密后的组播帧包括包括 IP 载荷 703 和 IP 首部 702 以及 ESP 首部 705，IP 首部 702 之前还可以包括链路层首部 701，如以太网首部。IP 载荷 703 包括的是密文的组播业务数据 704。ESP 首部 705 包括 SPI (Security Parameters Index, 全参数索引) 705A 和/或序列号 (Sequence Number) 705B。

接入控制子系统的 DEU A104 加密组播帧具体包括：

- 1、接收到组播帧，例如 DRU A107 接收到如图 6 所示的组播帧交给 DEU A104，DEU A104 解析组播帧，获取 IP 载荷部分保护的组播业务数据以及 IP 首部；

- 2、DEU A104 根据 IP 首部的目的 IP 和/或源 IP 作为组播流标识，获取该流标识对应的 MEK，使用指定的算法将组播业务数据和 MEK 进行计算得到密文组播业务数据；

- 3、创建 ESP 首部，包括生成 SPI 以及序列号域等，SPI 以及序列号可以作为 MEK 切换标记，A104DEU 可以通过改变 SPI 或序列号值指示 MEK 切换；

- 4、将明文组播帧的 IP 首部、新创建的 ESP 首部、密文组播业务数据按照标准的格式重组成组播帧，如图 7 所示的格式，详细重组格式请参见 RFC 标准，例如 RFC 2406，链路层首部可以是明文组播帧的链路层首部，也可以是重新构造的链路层首部。

用户子系统的 CDU B102 解密组播帧具体包括：

- 1、接收到密文组播帧，例如 ONU 接收到如图 7 所示的组播帧，解析组播帧以及获取 IP 载荷包含的密文组播业务数据、ESP 首部以及 IP 首部；

- 2、根据 IP 首部和/或 ESP 首部获取组播流标识，根据组播流标识获取解密的 MEK，然后将 MEK 和密文组播业务数据计算得到还原的明文组播业务数据，B102CDU 可以根据 IP 首部的 IP 地址或 SPI 或序列号值或时间戳获取

MEK;

3、将从密文组播帧得到的 IP 首部和明文组播数据等生成明文组播帧，链路层首部可以是密文组播帧的链路层首部，也可以是重新构造的链路层首部。

本发明实施例五详细描述采用吉比特的无源光网络（GPON）加密和解密组播帧的方法，如图 8 所示。在 GPON 应用中，OLT 可以加密吉比特的无源光网络封装（GEM）载荷或以太网载荷。GPON 组播帧包括物理层控制块（PCBd）和 GPON 的帧净荷。物理层控制块（PCBd）进一步包括物理层同步（Psync）和超帧指示（Ident），GPON 帧净荷包括 GEM 首部和 GEM 载荷，GEM 首部包括端口标识（PortID）和载荷指示（PTI），GEM 载荷包括以太网首部和以太网载荷，以太网首部包括目的地址和源地址，以太网载荷还进步一步可以包括 IP 首部和 IP 载荷。GPON 组播帧的流标识可以由下列参数中的至少一个组成：GEM 首部的端口标识（PortID）、以太网首部的目的地址、以太网首部的源地址、IP 首部的目的地址、IP 首部的源地址等。超帧指示（Ident）包括了帧计数器，超帧指示可以用于帧的 MEK 切换标记。

本发明实施例六详细描述采用吉比特的无源光网络（GPON）使用 OAM 消息分发和切换 MEK 的消息，如图 9 所示，OAM 的帧结构，其包括：ONU 标识（ONU-ID）、消息标识（Message-ID）、数据（data）及循环冗余码（Cyclic Redundancy Code，CRC）。MEK 分发消息格式见表 3：

表 3 MEK 分发消息格式

字节编号	内容	描述
1	ONU-ID	指示发起此消息的 ONU
2	Xx	表明消息为 MEK 分发消息
3..12	MEK 信息	MEK 索引、MEK 值、MEK 对应的流标识
MEK信息具体封装格式视具体实现而定，MEK信息可以使用多个 OAM消息携带。		

MEK 切换消息格式见表 4：

表 4 MEK 切换消息格式

字节编号	内容	描述
1	ONU-ID 或 11111111	向指定ID对应的ONU发送的消息或者所有ONU发送的消息。向所有ONU广播的消息时，ONU-ID=0xFF。
2	YY	表明消息为MEK切换消息
3-12	切换标记	MEK切换标记（如super frame number）和/或组播流标识。

本发明实施例七详细描述采用以太网的无源光网络（EPON）使用 OAM 消息分发和切换 MEK 的消息，如图 10 所示，EPON 采用 OAM 实现 MEK 分发或切换消息的帧结构，包括：目的地址、源地址、消息类型、组播流标识、MEK。目的地址为用户子系统的 ONU 地址，源地址为 OLT 地址、消息类型用于识别 MEK 分发或切换消息、组播流标识包括组播地址、LLD 等。

本发明的实施例中，在广播式（共享介质）接入应用中，授权用户才能使用组播业务数据，防止非法用户使用组播业务。加强了在共享介质接入的组播安全控制，杜绝了未授权或恶意访问，保护了运营商的投资。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

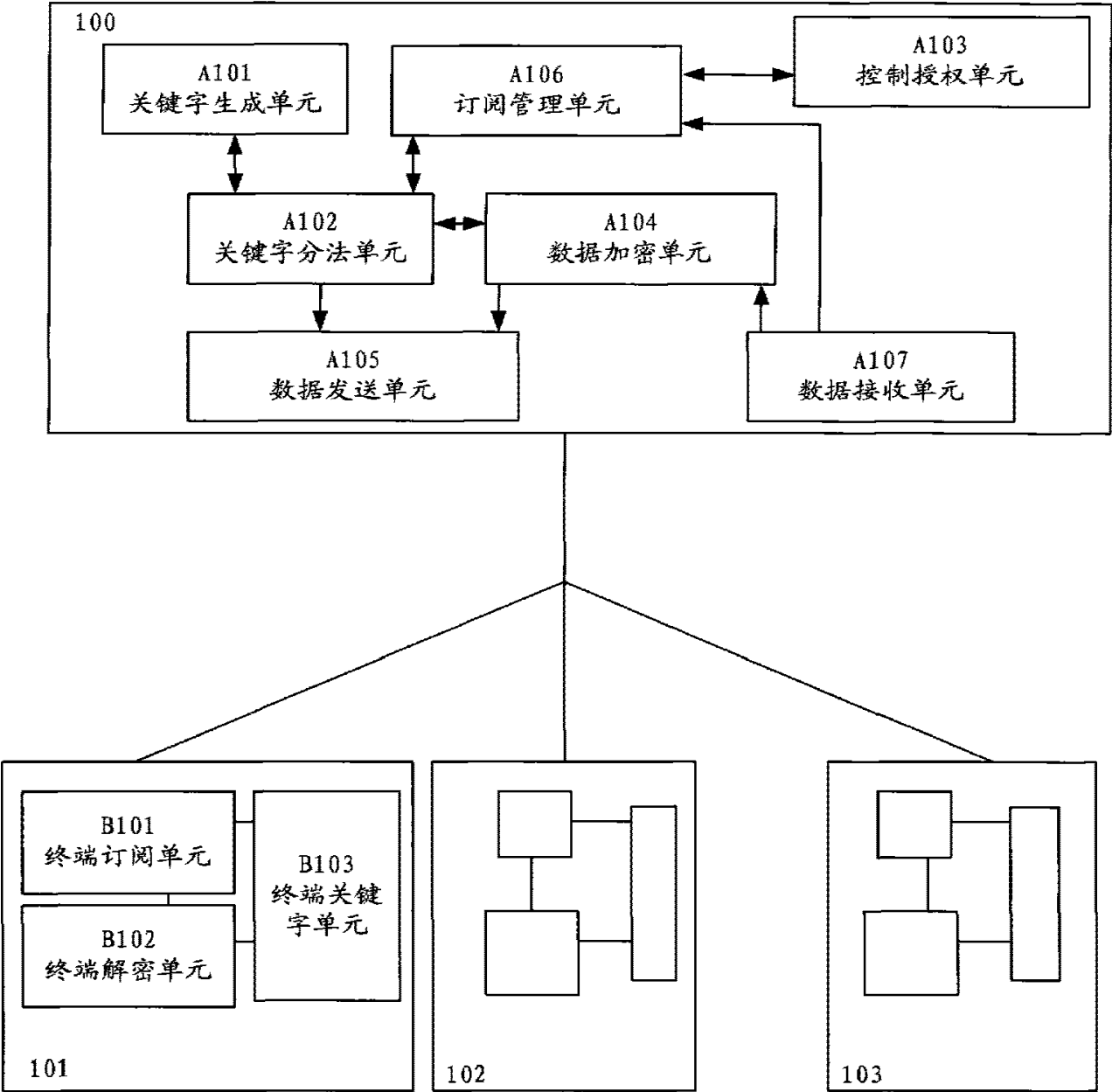


图 1

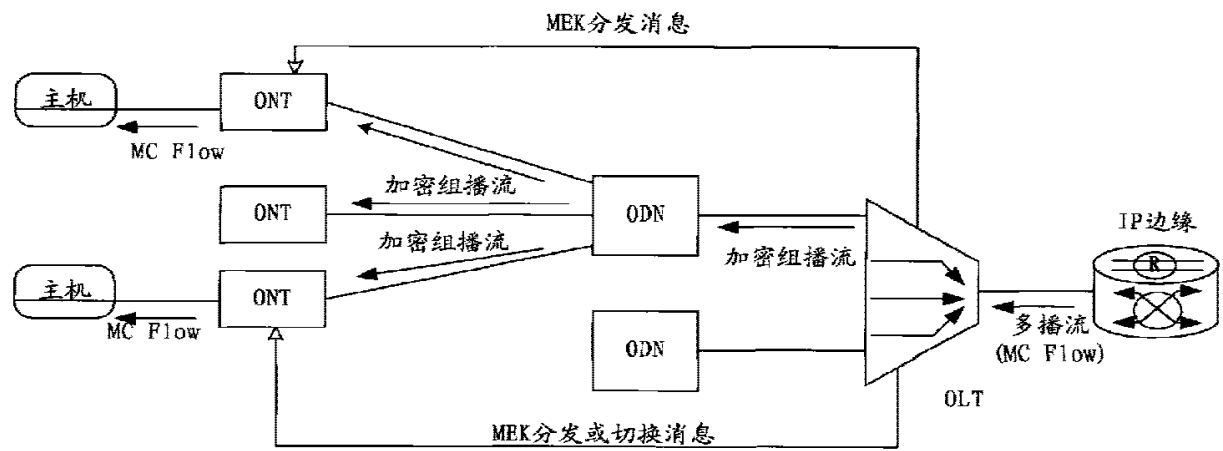


图 2

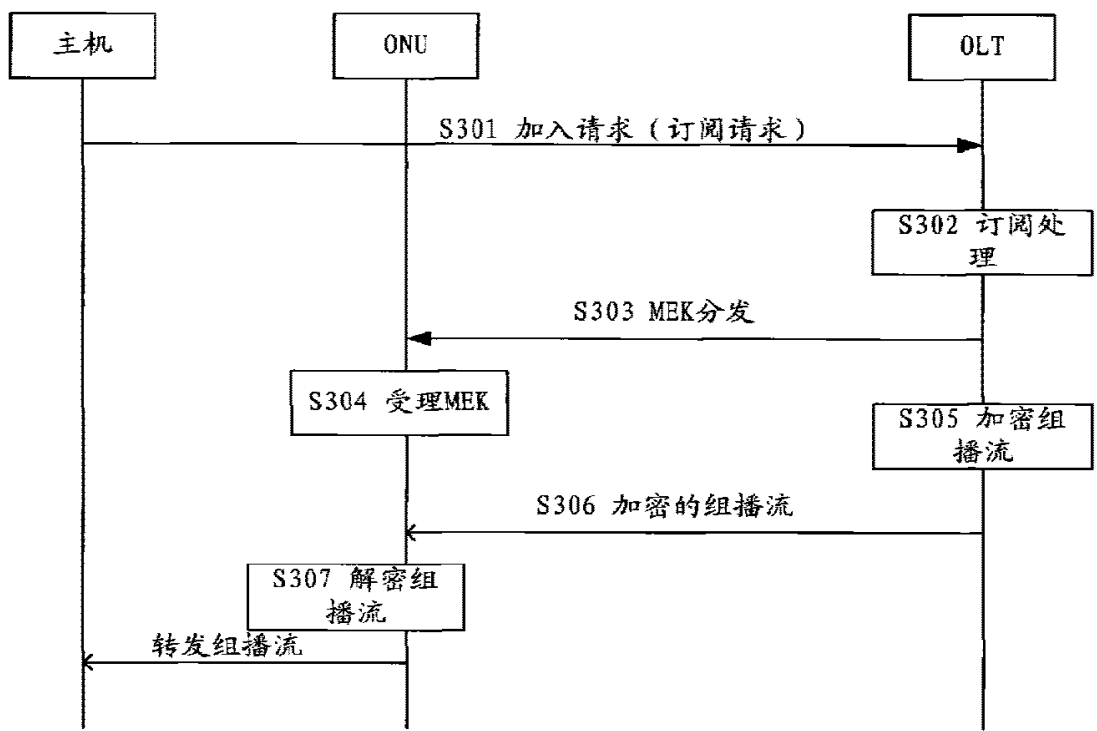


图 3

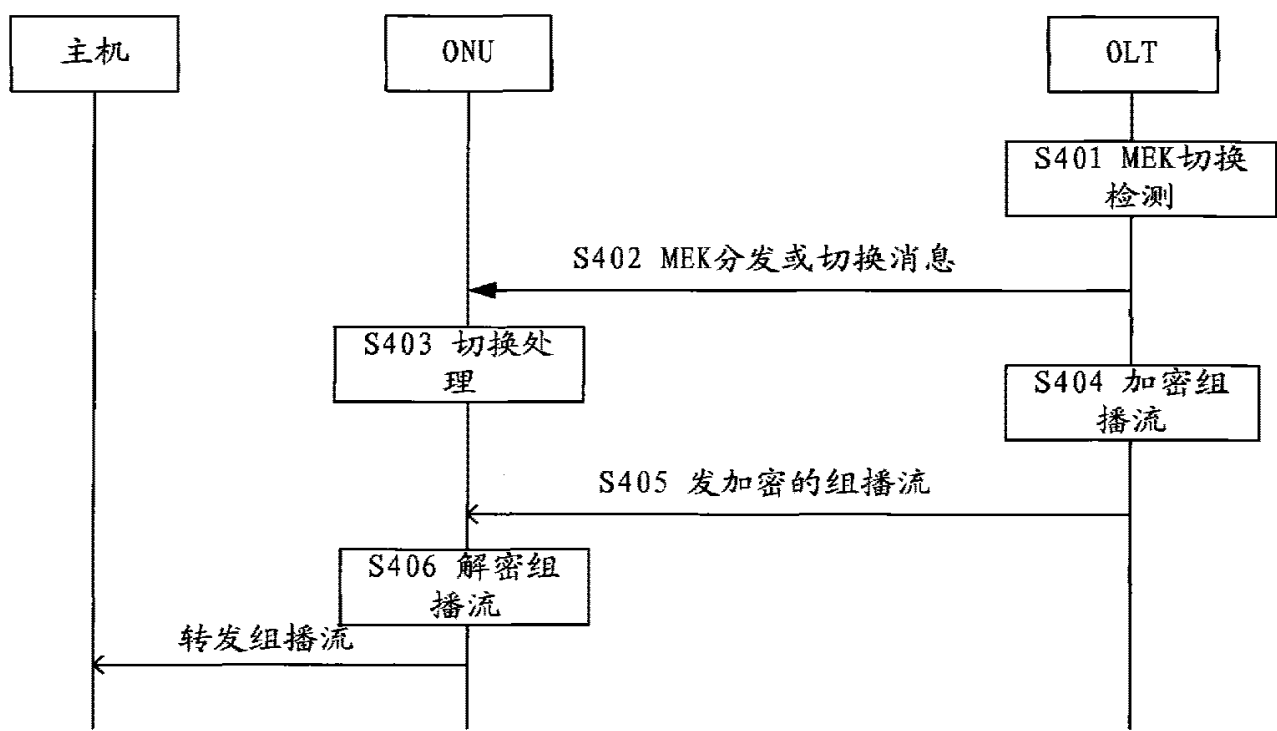


图 4

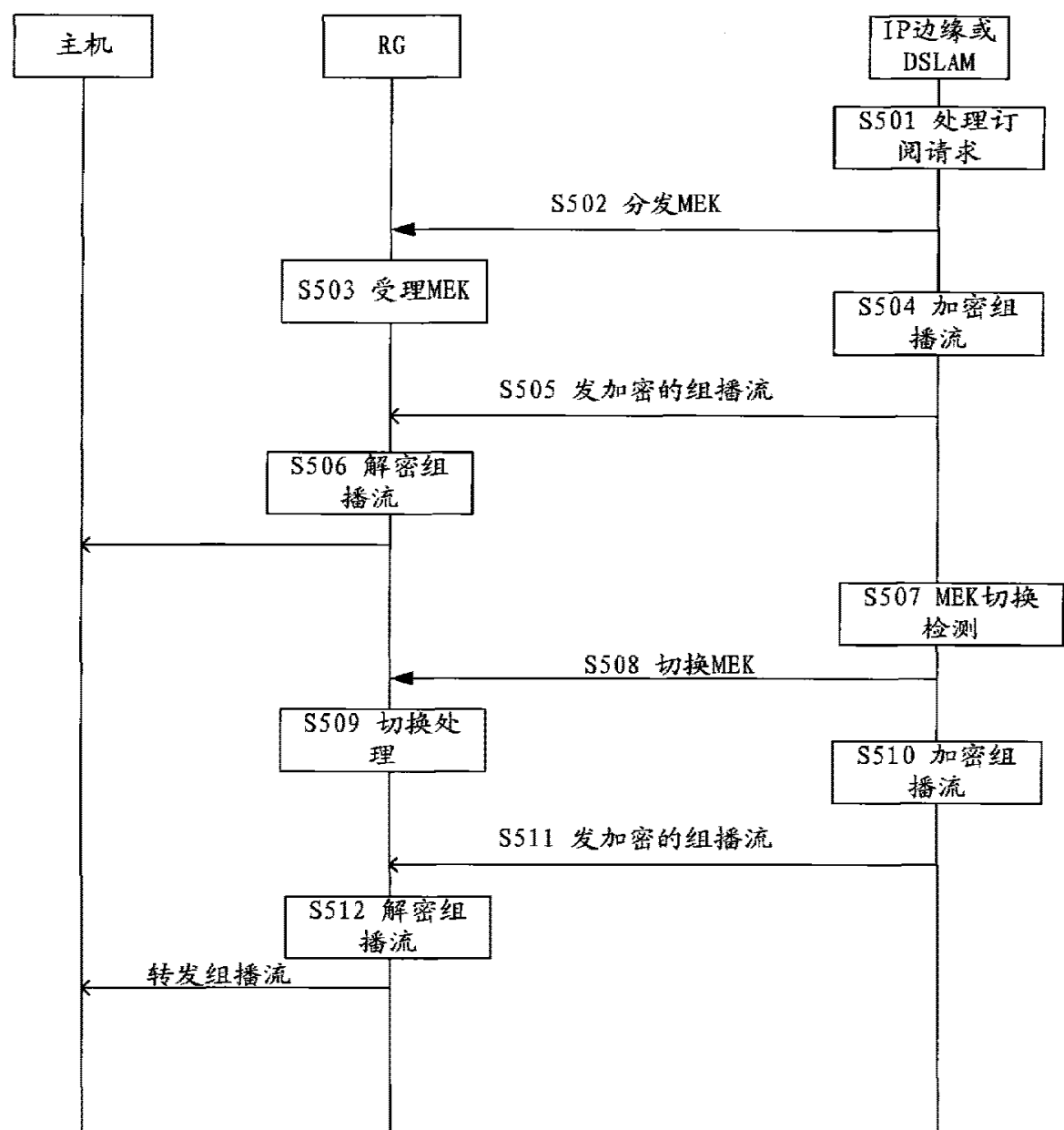


图 5

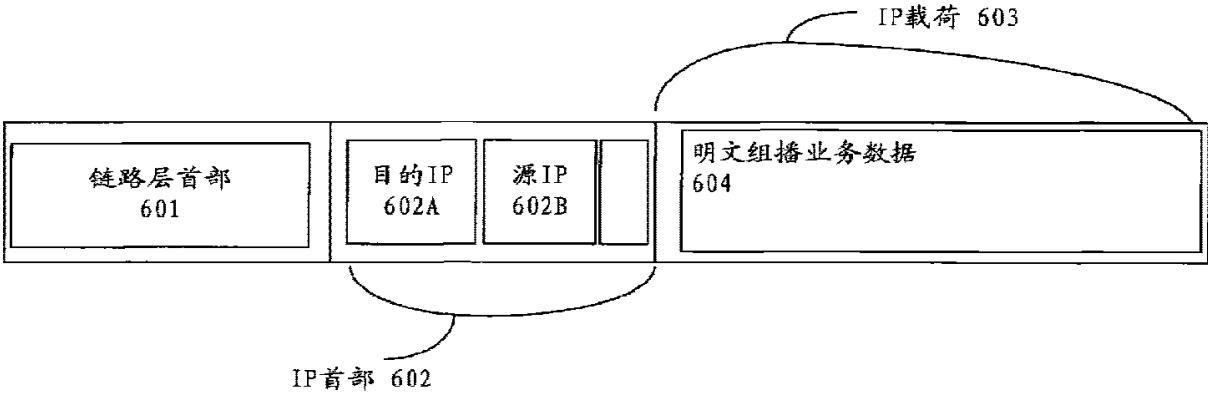


图 6

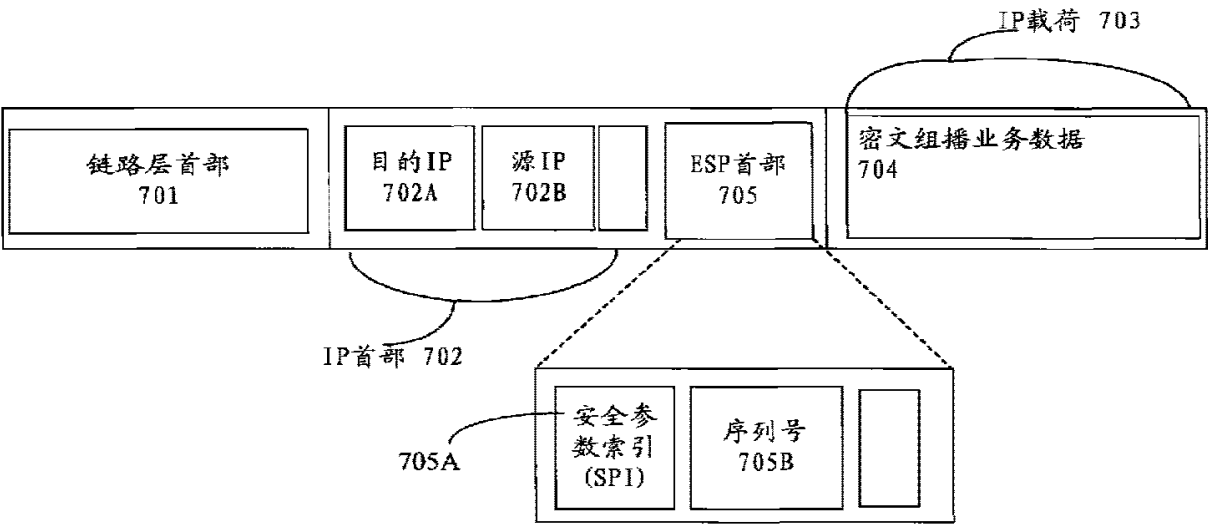


图 7

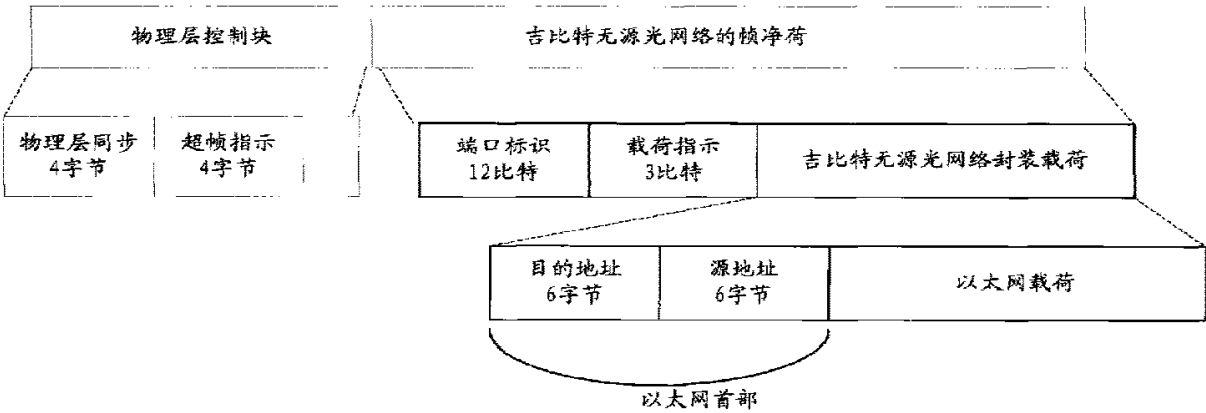


图 8

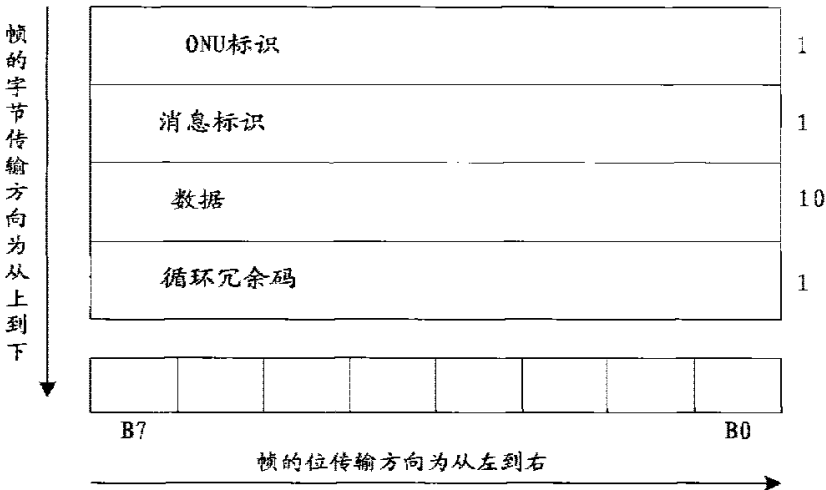


图 9

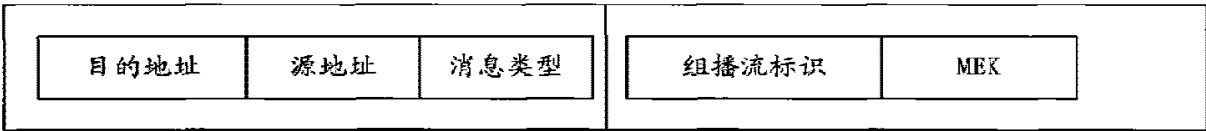


图 10

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/257,731	Filing Date 09/20/2011	☐ To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

	(Column 1)	(Column 2)	(Column 3)	(Column 4)	(Column 5)	RATE (\$)	ADDITIONAL FEE (\$)	
AMENDMENT	05/10/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			
	Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0	x \$80 =	0	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	x \$420 =	0	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
						TOTAL ADD'L FEE	0	

	(Column 1)	(Column 2)	(Column 3)	(Column 4)	(Column 5)	RATE (\$)	ADDITIONAL FEE (\$)	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =		
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =		
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
						TOTAL ADD'L FEE		

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DONNA 1. SMALLS LOGAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Amendments to the claims:

This listing of claims will replace all prior versions, and listings, of the claims in the application.

Listing of Claims:

1. (Currently amended) A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a ~~public~~keycommon key, and using the ~~public~~keycommon key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same ~~public~~keycommon key to carry out encryption; and

said OLT sending the ~~public~~keycommon key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

2. (Currently amended) The method of claim 1, further comprising:

after obtaining the ~~public~~keycommon key, said ONU using said ~~public~~keycommon key to decrypt the multicast service data, which the ONU applies to receive, in the bearer channel.

3. (Currently amended) The method of claim 1, further comprising:

said OLT generating the ~~public~~keycommon key and setting an aging time for the ~~public~~keycommon key, and after the aging time arrives, it regenerating a new ~~public~~keycommon key, and using the new ~~public~~keycommon key to encrypt the multicast service data in the bearer channel, and sending the new ~~public~~keycommon key to the ONU that is activated successfully and applies for the multicast service data.

4. (Currently amended) The method of claim 1, wherein:

the step of said OLT sending the ~~public key~~common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the ~~public key~~common key applied in encrypting the multicast service data to said ONU; or

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the ~~public key~~common key applied in encrypting said multicast service data to the ONU.

5. (Currently amended) The method of claim 1, wherein:

the multicast service data in different bearer channels use different ~~public key~~common keys or the same ~~public key~~common key.

6. (Currently amended) The method of claim 1, wherein:

in the step of said OLT sending the ~~public key~~common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the ~~public key~~common key.

7. (Currently amended) A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a ~~public key~~common key;

said encryption unit is configured to: encrypt multicast service data born in a same one bearer channel with a same ~~public key~~common key;

said sending unit is configured to: send the encrypted multicast service data, and send the ~~public key~~common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

8. (Currently amended) The device of claim 7, wherein,

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the ~~public key~~common key, and when the aging time arrives, notifying said key generation unit to regenerate a ~~public key~~common key.

9. (Currently amended) The device of claim 7, wherein:

said sending unit is configured to apply following methods to send the ~~public key~~common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the ~~public key~~common key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast service data, and then sending the ~~public key~~common key applied in encrypting the multicast service data to the ONU.

10. (Currently amended) The device of claim 7, wherein,

said sending unit is also configured to: send the ~~public key~~common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the ~~public key~~common key.

11. (Currently amended) The method of claim 2, further comprising:

said OLT generating the ~~public key~~common key and setting an aging time for the ~~public key~~common key, and after the aging time arrives, it regenerating a new ~~public key~~common key, and using the new ~~public key~~common key to encrypt the multicast service data in the bearer channel, and sending the new ~~public key~~common key to the ONU that is activated successfully and applies for the multicast service data.

12. (Currently amended) The method of claim 2, wherein:

in the step of said OLT sending the ~~public key~~common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a

bearer channel identification of the bearer channel where all multicast service data are encrypted with the ~~public key~~common key.

13. (Currently amended) The device of claim 9, wherein,
said sending unit is also configured to: send the ~~public key~~common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the ~~public key~~common key.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	Customer No.: 95957
ZHANG, Dezhi et al.	)	
Serial No.: 13/257,731	)	Confirmation No.: 6831
Filed: 09/20/2011	)	
For: Method and Device for Encrypting	)	Art Unit: 2492
Multicast Service in Passive Optical Network	)	
System	)	Examiner: KORSAK, OLEG

Amendments and Response to Non-final Office Action

Dear Sir / Madam,

Responsive to the non-final Office Action dated February 14, 2013, Applicants submit the following amendments and remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable, and the application be allowed.

Amendments made to the Abstract are reflected in page 2 of this paper.

Amendments made to the claims are reflected in the listing of the claims, which begins on page 3 of this paper.

Remarks begins on page 7 of this paper.

Conclusion begins on page 11 of this paper.

Amendments to the Abstract

Please replace the Abstract with following paragraph:

A method for encrypting multicast services in a passive optical network system is provided in the present invention, and the method includes: an Optical Line Terminal (OLT) generating a public key, and using the public key to encrypt the multicast service data in a bearer channel and then transmitting the encrypted data, the multicast service data in the same one bearer channel being encrypted using the same public key; and said OLT sending the public key, which is used to encrypt the multicast service data, via a management control channel to an Optical Network Unit (ONU) which is activated successfully and requests to receive said multicast service data. A device for encrypting multicast services in a passive optical network system is also provided in the present invention. ~~By applying the bearer channel encryption mechanism, the present invention is able to reduce the complexity of the OLT encryption mechanism and the ONU decryption mechanism on the premise of ensuring the encryption of the multicast services.~~

Electronic Acknowledgement Receipt

EFS ID:	15747549
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	10-MAY-2013
Filing Date:	20-SEP-2011
Time Stamp:	16:04:43
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Response_to_1stOA_AFD111101435-US.pdf	180483 27587fa27716d5f603b8d0d6bd693d5533da46d5	no	11

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REMARKS

The non-final Office Action dated February 14, 2013 has been carefully reviewed and the following amendments and remarks are responsive thereto. The abstract and claims 1-13 are amended.

No new matter is added.

Claims 1-13 remain pending. Reconsideration and allowance are respectfully requested.

Specification

The abstract has been amended to have less than 150 words.

Claim Rejections - 35 USC § 112

The claims 1-13 are rejected under 35 U.S.C. 112 (b) because the term "public key" in claims 1-13 is used by the claim to mean "common key".

Without agreeing with or acquiescing to the rejection, Applicant has amended claims 1-13 to replace the "public key" in claims 1-13 with "common key" in an attempt to expedite prosecution. Applicant requests that this rejection be withdrawn.

Claim Rejections - 35 USC § 102

Claims 1, 2, 4-7, 9, 10, 12, 13 are rejected under 35 U.S.C. 102(b) as being anticipated by HE (CN 1855834 November 1, 2006, translation by Dialog).

The rejections are respectfully traversed based on the above amendment and the following remarks.

Regarding independent claim 1

HE fails to disclose all of the limitations of claim 1. More particularly, claim 1 recites:

“A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a ~~public key~~common key, and using the ~~public key~~common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same ~~public key~~common key to carry out encryption; and

said OLT sending the ~~public key~~common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.”

HE fails to disclose at least the distinctive features of “common key to encrypt multicast service data in a **bearer channel**” in claim 1 of present application.

In the Office Action, the Examiner indicated that the Abstract of HE discloses the feature “... using the ~~public key~~common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a same one bearer channel using a same ~~public key~~common key to carry out encryption;...”.

Applicants respectfully disagree.

The reference HE discloses “the public key is used to encrypt multicast bit-stream” according to the office action and the Abstract of HE.

However, the people with ordinary skill in the art would recognize that the bear channel is different from the multicast bit-stream. There may be multiple multicast bit-streams in one bear channel. The key used to encrypt data in a multicast bit-stream is different from the key used to encrypt data in a bearer channel which may comprise multiple multicast bit-streams.

Therefore, the reference HE fails to teach the same elements and same functions of the elements with the ones in claim 1.

According to MPEP 2131, to anticipate a claim, the reference must teach every element of the claim either expressly or inherently, described, in a single prior art reference. Since the reference **HE** does not teach every element of the amended claim 1, the applicants respectively submit that the claim 1 of the present application is not anticipated by the reference **HE** under

35 U.S.C. 102(b). Applicants request reconsideration and withdrawal of the 35 USC § 102 rejection to claim 1.

Regarding Independent Claim 7

Claim 7 disclose an apparatus that implements the method disclosed in claim 1. In light of above, claim 7 is allowable over HE for at least the same reason as claim 1, and more specifically for the specific features it recites.

Regarding claims 2, 4-6, 9, 10, 12 and 13

Claims 2, 4-6, 9, 10, 12 and 13 depend on claims 1 or 7. In light of above, claim 2, 4-6, 9, 10, 12 and 13 are also allowable over HE for at least the same reason as claim 1 or 7 from which the depend, and more specifically for the specific features they recite.

Claim Rejections - 35 USC § 103

The office action rejected claims 3, 8 and 11 under 35 U.S.C. 103(a) as being unpatentable over HE (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang (CN 1866857 November 22, 2006, translation by Dialog).

The rejections are respectfully traversed based on the above amendment and the following remarks.

Regarding claims 3 and 8

In light of the analysis for the claim 1, HE fails to disclose at least the distinctive features of “common key to encrypt multicast service data in a **bearer channel**” in claim 1 of present application. For at least the same reason, HE fails to teach, suggest or render obvious all of limitations of claim 3 which depends on claim 1.

Jiang is not able to cure at least these deficiencies of HE as well.

Therefore HE and Jiang, alone or in any proper combination, fails to teach, suggest or render obvious all of limitations of claim 3.

In light of above, claim 3 is allowable over HE alone, or in any proper combination with Jiang for at least the same reasons as claim 1 from which it depends, and more specifically for the specific features it recites.

Claim 8 disclose an apparatus that implement the method disclosed in claim 3. In light of above, claim 8 is allowable over HE in view of Jiang for at least the same reason as claim 1 and 3, and more specifically for the specific features it recites.

Regarding claim 11

In light of the above, claim 11 is allowable over HE alone, or in any proper combination with Jiang for at least the same reasons as claim 1 from which it depends, and more specifically for the specific features it recites.

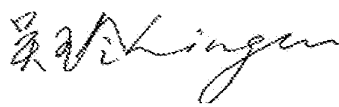
Conclusion

The Applicants believe they have responded to each matter raised by the Examiner. Allowance of the claims is respectfully solicited. It is believed that the present patent application, after the above amendments and statement of opinions, has overcome all the defects pointed out by the Examiner and is in conformity with the relevant provisions, so it should be granted patent rights.

The Applicants expect early granting of patent right for this application. If there is still a problem that the Examiner believes is not overcome by the above amendments and statement of opinions, please give the Applicants another chance to make amendments and further clarification or explanation or observation.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below. Favorable action is respectfully requested.

Respectfully submitted,

By: 

Ling Wu

Patent Agent for Applicant

Registration No. 66,304

Date: May 10, 2013
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854
(301) 301-637-2202
(301) 251-0237 (fax)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	06/14/2013		
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			EXAMINER KORSAK, OLEG	
			ART UNIT 2492	PAPER NUMBER
			MAIL DATE 06/14/2013	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/257,731	Applicant(s) ZHANG ET AL.	
	Examiner OLEG KORSAK	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 10 May 2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5) ☒ Claim(s) 1-13 is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☒ Claim(s) 1-13 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some * c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This action is in response to amendment filed on May 10, 2013 for the application # 13/257,731 filed on September 20, 2011.

By this amendment, claims 1-13 are amended. Accordingly, claims 1-13 are pending, and are directed toward a METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM.

Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) The invention was patented or described in a printed commonation in this or a foreign country or in common use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 4-7, 9, 10, 12, 13 are rejected under 35 U.S.C. 102(b) as being *anticipated* by He (CN 1855834 November 1, 2006, translation by Dialog), hereinafter referred to as He.

As per **claim 1**, He teaches a method for encrypting multicast service in a passive optical network system (*a passive optical network pon technology, He, page 2*), the method comprising: an optical line terminal (OLT) generating a common key (*means of generating a key at the optical network line terminal, He, ABSTRACT*), and using the common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in a

same one bearer channel using a same common key to carry out encryption (*said key is used as the common key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT*); and said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data (*while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream. He, ABSTRACT*).

As per **claim 2**, He teaches the method of claim 1, further comprising: after obtaining the common key, said ONU using said common key to decrypt the multicast service data, which the ONU applies to receive, in the bearer channel (*And the key by using the other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal using the key to multicast data stream decoding receives the multicast data stream. He, Page 3*).

As per **claim 4**, He teaches the method of claim 1, wherein: the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises: the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU (*Can firstly the optical network user end of the optical network line terminal sends multicast application of optical network line*

road terminal to the multicast request processing according to user authority is determined whether to the optical network user end distributing multicast. If the user does not multicast authority optical network line terminal is not the multicast request. He, Page 3).

As per **claim 5**, He teaches the method of claim 1, wherein: the multicast service data in different bearer channels use different common keys or the same common key *(By using this invention using the same service channels as same as the port id or vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6).*

As per **claim 6**, He teaches the method of claim 1, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key *(and the distribution of the multicast occupies a downlink service channel by channel number port id virtual channel identifier vpi or virtual channel identifier address to identify vci port is id. He, Page 5).*

As per **claim 12**, He teaches the method of claim 2, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key *(the same service channels as same as the port id or vpi/vci of Service channel for the same multicast user transmitting multicast encrypted data streams. He, Page 6).*

Apparatus **claims 7, 9, 10, 13** are drawn to the apparatus corresponding to the method of using the same as claimed in claims 1, 2, 4-6, 12. Therefore apparatus claims 7, 9, 10, 13 correspond to method claims 1, 2, 4-6, 12, and are rejected for the same reasons of anticipation as used above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang (CN 1866857 November 22 2006, translation by Dialog), hereinafter referred to as He and Jiang respectively.

As per **claims 3 and 8**, He does not teach the aging time, Jiang, however, teaches the method of claim 1 further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (*that receiver the user, OLT distributed of downlink service channel and a common key for user ONT, and timing updating the common downlink service channel and a common key, Jiang, ABSTRACT*).

He in view of Jiang are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang, p.4].

As per **claim 11**, He does not teach the aging time, Jiang, however, teaches the method of claim 2, further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (Steps: 14 OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, and starting timing, wherein the output of downlink service channel and a key, overtime. The gaining the group multicast data stream of the user request, OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, a OLT generating the novel of downlink service channel number and a starting timing. Jiang, Page 4)

He in view of Jiang are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang, p.4].

Response to Arguments

Applicant's arguments with regards to claims 1-13 have been fully considered, but they are not persuasive.

“bearer channel” argument – As to claim 1, Applicant argues that HE fails to disclose at least the distinctive features of "common key to encrypt multicast service data in a bearer channel" in

claim 1 of present application. There may be multiple multicast bit-streams in one bear (sic) channel. The key used to encrypt data in a multicast bit-stream is different from the key used to encrypt data in a bearer channel which may comprise multiple multicast bit-streams (REMARKS, p.8).

Response – Examiners puts on record that Applicant admitted that HE teaches the key is used to encrypt at least one multicast bit-stream in a bearer channel. The limitation “the multicast service data in different bearer channels use different public keys or the same public key” is claimed by applicant in dependent claim 5 and met by reference of HE “By using this invention using the same service channels as same as the port id or vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6.” [NFOAM 02/14/2013, page 5). The limitation “of the bearer channel where all multicast service data are encrypted with the public key” is claimed by applicant in dependent claim 6 and met by reference of HE “and the distribution of the multicast occupies a downlink service channel by channel number port id virtual channel identifier vpi or virtual channel identifier address to identify vci port is id. He, Page 5.” [NFOAM 02/14/2013, page 6).
Conclusion -Therefore, in view of the above reasons, Examiner maintains rejections.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSAK whose telephone number is (571)270-1938. The examiner can normally be reached on Monday-Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Common PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/O. K./

Examiner, Art Unit 2492

/Saleh Najjar/

Supervisory Patent Examiner, Art Unit 2492

<i>Index of Claims</i> 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	02/07/2013	06/05/2013						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731	
	Filing Date		2012-01-06	
	First Named Inventor	Dezhi Zhang et al.		
	Art Unit	2492		
	Examiner Name	KORSAK, OLEG		
	Attorney Docket Number	AFD111101435-US		

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20060031936	A1	2006-02-09	Enterasys Networks, Inc.			
	2	20070133800	A1	2007-06-14	Electronics & Telecommunications Research Institute			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	101547086	CN	A	2009-09-30	HUAWEI TECHNOLOGIES CO., LTD.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13257731
	Filing Date		2012-01-06
	First Named Inventor	Dezhi Zhang et al.	
	Art Unit	2492	
	Examiner Name	KORSAK, OLEG	
	Attorney Docket Number	AFD111101435-US	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	CN101547086A; Automatically Translated by the Intellectual Property Publishing House of SIPO, March 21, 2013 see pages 1-12	☐
	2	XP11382244, ON EPON SECURITY ISSUES; The Electronic Magazine of Original Peer-Reviewed Survey Articles;1ST QUARTER 2007, VOLUME 9, NO.1; pages 68-83.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Oleg Korsak/	Date Considered	06/05/2013
--------------------	---------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2012-01-06
First Named Inventor	Dezhi Zhang et al.
Art Unit	2492
Examiner Name	KORSAK, OLEG
Attorney Docket Number	AFD111101435-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ling Wu/	Date (YYYY-MM-DD)	2013-04-26
Name/Print	Ling Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /O.K

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a common key, and using the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in ~~a~~ the same one bearer channel ~~using~~ use a same common key to carry out encryption; and

said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

2. (Currently Amended) The method of claim 1, further comprising:

after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel.

3. (Previously Presented) The method of claim 1, further comprising:

said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

4. (Previously Presented) The method of claim 1, wherein:

the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU.

5. (Previously Presented) The method of claim 1, wherein:

the multicast service data in different bearer channels use different common keys or the same common key.

6. (Previously Presented) The method of claim 1, wherein:

in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

7. (Currently Amended) A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a common key;

said encryption unit is configured to: encrypt multicast service data of all multicast services born in a same one bearer channel with a same common key;

said sending unit is configured to: send the encrypted multicast service data, and send the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

8. (Previously Presented) The device of claim 7, wherein,

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the common key, and when the aging time arrives, notifying said key generation unit to regenerate a common key.

9. (Previously Presented) The device of claim 7, wherein:

said sending unit is configured to apply following methods to send the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the common key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast service data, and then sending the common key applied in encrypting the multicast service data to the ONU.

10. (Previously Presented) The device of claim 7, wherein,

said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

11. (Previously Presented) The method of claim 2, further comprising:

said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

12. (Previously Presented) The method of claim 2, wherein:

in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

13. (Previously Presented) The device of claim 9, wherein,

said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dezhi Zhang et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **2492**

) Examiner: **KORSAK, OLEG**

Amendments and Response to Final Office Action

Dear Sir / Madam,

Responsive to the final Office Action dated June 14, 2013, Applicants submit the following remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable. Favorable reconsideration of the application and withdrawal of the rejections is respectfully requested.

Amendments to the Claims are reflected in the listing of the claims, which begins on page 2 of this paper.

Remarks begins on page 6 of this paper.

Conclusion begins on page 10 of this paper.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dezhi Zhang et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **2492**

) Examiner: **KORSAK, OLEG**

)

Amendments and Response to Final Office Action

Dear Sir / Madam,

Responsive to the final Office Action dated June 14, 2013, Applicants submit the following remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable. Favorable reconsideration of the application and withdrawal of the rejections is respectfully requested.

Amendments to the Claims are reflected in the listing of the claims, which begins on page 2 of this paper.

Remarks begins on page 6 of this paper.

Conclusion begins on page 10 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	16561002
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	12-AUG-2013
Filing Date:	20-SEP-2011
Time Stamp:	13:36:06
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	Response_to_FOA_AFD111101435-US.pdf	192677 847a25116ce87af1031194939aabe1b56742ebdd	no	10

Warnings:

Information:

2	After Final Consideration Program Request	AFCP20_sb0434_AFD111101435-US.pdf	226524 44ad9d76eba82a4b28c74b4b1f447573be9135fd	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				419201	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0		
Practitioner Docket No.: AFD111101435-US	Application No.: 13/257,731	Filing Date: 09/20/2011
First Named Inventor: Dezhi Zhang	Title: Method and Device for Encrypting Multicast Service in Passive Optical Network System	
<p>APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.</p> <ol style="list-style-type: none"> 1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (<i>e.g.</i>, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c). 2. The above-identified application contains an outstanding final rejection. 3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect. 4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection. 5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response. 6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web). 7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.] 8. By filing this certification and request, applicant acknowledges the following: <ul style="list-style-type: none"> • Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0. • The examiner will verify that the AFCP 2.0 submission is compliant, <i>i.e.</i>, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions: <ul style="list-style-type: none"> ○ The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, by mailing an advisory action. ○ If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview. <ul style="list-style-type: none"> ▪ The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate. ▪ If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116. 		
Signature /Ling Wu/	Date 8/12/2013	
Name (Print/Typed) Ling Wu	Practitioner Registration No. 66,304	
<p>Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.</p>		
☐ * Total of <u>1</u> forms are submitted.		

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

REMARKS

The final Office Action dated June 14, 2013, has been carefully reviewed and the following amendments and remarks are responsive thereto. Claims 1, 2 and 7 are amended.

No new matter is added.

Claims 1-13 remain pending. Reconsideration and allowance are respectfully requested.

Claim Rejections - 35 USC § 102

The Office Action rejected claims 1, 2, 4-7, 9, 10, 12, 13 under 35 U.S.C. 102(b) as being anticipated by He (CN 1855834 November 1, 2006, translation by Dialog), hereinafter referred to as He.

Claims 1, 2 and 7 of the present application have been amended.

The Applicants respectfully traverse the rejection based on above amendments and following remarks:

Claim 1

He fails to disclose at least the following limitations of the amended claim 1. More particularly, the amended claim 1 recites:

“A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a common key, and using the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in a the same one bearer channel using use a same common key to carry out encryption; and

said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.”

Claim 1 of the present application is amended. One skilled in the art knows that one bearer channel can include a plurality of service channels to bear different multicast services; thus, in order to define the claim 1 more clearly, the Applicants amend claim 1 of “using the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in ~~a the~~ same one bearer channel ~~using~~ use a same common key to carry out encryption”

No new matter has been added.

Applicants disagree the Examiner's point of view that “HE teaches the key is used to encrypt at least one multicast bit-stream in a bearer channel” on page 7 of the final Office Action. In HE, it discloses to encrypt the multicast data stream in **one** service channel (step A3 on page 3, lines 23-24 on page 4, step 4-2) on page 5, etc.), does **not** disclose any information about more than one service channel and further does **not** disclose any information about the bear channel at all; and from the description of HE, there is no prompt for encrypt all multicast data streams, it only disclose that the key (**not different multicast data streams**) is transmitted using different service channels to different users in the same multicast group (lines 18-19 on page 6). Thus, HE does not teach the key is used to encrypt at least one multicast bit-stream in a bearer channel.

Based on the above analysis, the amended claim 1 defines that: the OLT generates a common key, and uses the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in the same one bearer channel use the same common key to carry out encryption.

In contrast, HE's invention provides a method for realizing multicast in PON, in which the OLT allocates the multicast service which is applied for to occupy one downlink service channel, and the OLT generates one key for this multicast service. (HE, steps A1-A3 on page 3)

It can be seen, HE's solution is only to "encrypt the multicast data stream in **one** service channel". But in HE, it does **not** disclose using the same common key to carry out encryption for the multicast service data of all multicast services in the same one bearer channel.

Therefore, HE fails to disclose at least the feature “using the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in ~~a~~ the same one bearer channel ~~using~~ use a same common key to carry out encryption” defined in the amended claim 1 of the present application.

Because HE does not teach each and every element of amended claim 1, the amended claim 1 is allowable over HE. (*See* MPEP 2131)

Claim 2

The amended claim 2 further defines the feature “after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel”, which are not disclosed by HE also.

Specifically, because the multicast service data of all multicast services in the same one bearer channel use a same common key to carry out encryption, after the ONU obtains the common key, it can decrypt all the multicast service data in the same bearer channel using the common key; that is to say, there is no need to generate different keys by the OLT for different multicast services in different service channels respectively. However, from the above analysis for HE, it discloses to encrypt the multicast data stream in **one** service channel (step A3 on page 3, lines 23-24 on page 4, step 4-2 on page 5, etc). Therefore, HE does not disclose the feature defined in the amended claim 2.

In light of the above, claim 2 is allowable over HE for at least the same reasons as the amended claim 1 from which it depends, and more specifically for the specific features it recites.

Claim 7

The amended claim 7 defines a device for encrypting multicast service in a passive optical network system corresponding to the amended claim 1.

In light of the above, the amended claim 7 is allowable over HE for at least the same reasons as the amended claim 1, and more specifically for the specific features it recites.

Claims 4-6, 9, 10, 12, 13

In light of the above, claims 4-6, 9, 10, 12, 13 are allowable over HE for at least the same reasons as the amended claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

Claim Rejections - 35 USC § 103

The Office Action rejected claims 3, 8 and 11 under 35 U.S.C. 103(a) as being unpatentable over HE (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang (CN 1866857 November 22, 2006, translation by Dialog), hereinafter referred to as He and Jiang respectively.

The Applicants respectfully traverse the rejections based on the following remarks.

Claims 3, 8 and 11

In light of above, claims 3, 8 and 11 are allowable over He alone, or in any proper combinations with Jiang, for at least the same reasons as the amended claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

Conclusion

The Applicants believe they have responded to each matter raised by the Examiner. Allowance of the claims is respectfully solicited. It is believed that the present patent application, after the above amendments and statement of opinions, has overcome all the defects pointed out by the Examiner and is in conformity with the relevant provisions, so it should be granted patent rights.

The Applicants expect early granting of patent right for this application. If there is still a problem that the Examiner believes is not overcome by the statement of opinions, please give the Applicants another chance to make amendments and further clarification or explanation or observation.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below. Favorable action is respectfully requested.

Respectfully submitted,


By: _____
Ling Wu
Patent Agent for Applicant
Registration No. 66,304

Date: August 12, 2013
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854
(301) 301-637-2202
(301) 251-0237 (fax)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	08/28/2013		
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			EXAMINER KORSAK, OLEG	
			ART UNIT 2492	PAPER NUMBER
			MAIL DATE 08/28/2013	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No. 13/257,731	Applicant(s) ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 12 August 2013 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance;
 (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires _____ months from the mailing date of the prior Advisory Action or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);

b) ☐ They raise the issue of new matter (see NOTE below);

c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

STATUS OF CLAIMS

14. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: 1-13.

Claim(s) withdrawn from consideration: _____.

/saleh najjar/ Supervisory Patent Examiner, Art Unit 2492	/OLEG KORSAK/ Examiner, Art Unit 2492
--	--

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's request for entry into AFCP 2.0 is acknowledged, but is denied because the response cannot be reviewed and a search conducted in the limited amount of time authorized for this pilot program. Therefore, the response is being reviewed under pre-pilot practice. The Applicant's arguments were already treated in FOAM (06/14/2013, pages 6-7. Applicant however continues to argue that "HE does not teach the key is used to encrypt at least one multicast bit-stream in a bearer channel" Examiner in addition to already provided references points to "By using this invention using the same service channels as same as the port id or vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6".

Conclusion -Therefore, in view of the above reasons, Examiner maintains rejections.

Electronic Patent Application Fee Transmittal				
Application Number:		13257731		
Filing Date:		20-Sep-2011		
Title of Invention:		Method and Device for Encrypting Multicast Service in Passive Optical Network System		
First Named Inventor/Applicant Name:		Dezhi Zhang		
Filer:		Ling Wu		
Attorney Docket Number:		AFD111101435-US		
Filed as Large Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for Continued Examination	1801	1	1200	1200
Total in USD (\$)				1200

**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)**

Application Number	13/257,731	Filing Date	2011-09-20	Docket Number (if applicable)	AFD111101435-US	Art Unit	2492
First Named Inventor	Dezhi Zhang			Examiner Name	KORSAK, OLEG		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 505648

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Ling Wu/	Date (YYYY-MM-DD)	2013-09-10
Name	Ling Wu	Registration Number	66304

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is a patent (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	16810403
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	10-SEP-2013
Filing Date:	20-SEP-2011
Time Stamp:	13:56:59
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1200
RAM confirmation Number	209
Deposit Account	505648
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Request for Continued Examination (RCE)	RCE_sb0030e_AFD111101435-US.pdf	697842 074007e59af6f9a059710296a9315d6a31490521	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30405 a2b72cac9f9624bad4d61a906767e94ce5043550	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			728247		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/257,731		Filing Date 09/20/2011		☐ To be Mailed	
---	--	--	--	--	---	--	----------------------------------	--	---------------------------------------	--

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

(Column 1)		(Column 2)				(Column 1)		(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)			FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A					
☐ SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A			N/A					
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A					
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*			X \$	=				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*			X \$	=				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))			If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL				

APPLICATION AS AMENDED – PART II

(Column 1)		(Column 2)		(Column 3)				(Column 1)		(Column 2)	
AMENDMENT	09/10/2013	CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)			ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0			X \$80 =			0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0			X \$420 =			0
☐ Application Size Fee (37 CFR 1.16(s))											
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE		0	

(Column 1)		(Column 2)		(Column 3)				(Column 1)		(Column 2)	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)			ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=			X \$			
	Independent (37 CFR 1.16(h))	*	Minus	***	=			X \$			
☐ Application Size Fee (37 CFR 1.16(s))											
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE			

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/VIKKI GRAY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Group key management protocol (GKMP) architecture

H Harney - Group, 1997 - tools.ietf.org

... Unlike normal parameter negotiation, where **common** security-level/range, and services are arrived at, the ... of the rekey will create the new **keys** in exactly the **same** manner as ... The classification labels used by the **key** management protocol should coincide with the labels used by ...

Cited by 649 Related articles All 6 versions Cite Save More

Multicast security: A taxonomy and some efficient constructions

R Canetti, J Garay, G Itkis, D Micciancio... - ... Joint Conference of ..., 1999 - ieeeexplore.ieee.org

... more efficient than regular MACs.) A very similar method allows for many senders to use the **same** structure of ... In Section 11 we list and discuss multicast security issues, in several **common** scenarios ... scheme the source uses $f_2 = 4e(w + 1) \ln(l/q)$ **keys** where each **key** is included ...

Cited by 910 Related articles All 48 versions Cite Save

System and method for secure group communications via multicast or broadcast

S Mitra - US Patent 5,748,736, 1998 - Google Patents

... 2 and 3 may be arranged by having the GSC or a TI server pass the **common** secret to ... Note that a secure multicast group and a network multicast group are not the **same** thing. ... Thus, there is a serious scaling problem with current published multicast **key** management techniques ...

Cited by 201 Related articles All 2 versions Cite Save

Iolus: A framework for scalable secure multicasting

S Mitra - ACM SIGCOMM Computer Communication Review, 1997 - dl.acm.org

... The advantage of using a **common** group **key** is that it obviates the need to separately ... and re-encrypting the packet is reduced to simply decrypting and re-encrypting the random **key**. ... At the **same** time receivers using an outdated KSGRP may accept data from senders who are ...

Cited by 896 Related articles All 18 versions Cite Save

Kronos: A scalable group re-keying approach for secure multicast

S Setia, S Koussih, S Jajodia... - Security and Privacy, ..., 2000 - ieeeexplore.ieee.org

... This **key** will be used to **encrypt** the group wide data **encryption key** when it is sent to ... If the interval between re-**keys** is large, this latency may be unacceptable for some applications. ... This is because employing the **same key** for a long period of time increases the chances of that ...

Cited by 314 Related articles All 10 versions Cite Save

IP multicast channels: EXPRESS support for large-scale single-source applications

HW Holbrook, DR Cheriton - ACM SIGCOMM Computer Communication ..., 1999 - dl.acm.org

... ncls (S,E) and (S',E) are unrelated, despite the **common** destination address. ... PIM-SM encounters the **same** delay-state tradeoff as EXPRESS, providing a choice between the ... The **key** difference is that EXPRESS provides application control of the policy for switching between ...

Cited by 390 Related articles All 61 versions Cite Save

HiperLAN/2—The broadband radio transmission technology operating in the 5 GHz frequency band

M Johnsson - HiperLAN/2 Global Forum, 1999 - iesparearques.net

... Broadcast and multicast traffic can also be protected by **encryption** through the use of **common keys** (all MTs associated to the **same** AP use the **same key**). **Common keys** are distributed **encrypted** through the use of the unicast **encryption key**. ...

Cited by 140 Related articles All 13 versions Cite Save More

Using AVL trees for fault-tolerant group key management

O Rodeh, KP Birman, D Dolev - International Journal of Information ..., 2002 - Springer

... The partition model is more general than the more **common** "crash failure" model since crash failures may be ... in the tree that "match"; ie, when pulled together they make a tree that is the **same** as a ... Clearly, the naive protocol builds **key** graphs for groups of members of size $2n$

Cited by 69 Related articles All 22 versions Cite Save

Key establishment for IGMP authentication in IP multicast

T Hardjono, B Cain - Universal Multiservice Networks, 2000. ..., 2000 - ieeeexplore.ieee.org

... the **Key** Server also provides the Access-Token to the Receiver through the **same** secure **channel**. ... special to the current scenario, and can only be resolved if public **key** certificates are ... In this paper we have discussed a method for delivering cryptographic **keys** to host-members ...

Cited by 45 Related articles All 2 versions Cite Save

The multicast group security architecture

T Hardjono, B Weis - 2004 - tools.ietf.org

... The requirement that policy translation results in the **same** objects places constraints on the use and representations in the high-level policies. ... **Key** Servers and group members may take advantage of a **common** Public **Key** Infrastructure (PKI) for increased scalability of ...

Cited by 149 Related articles All 4 versions Cite Save More

Notice of References Cited	Application/Control No. 13/257,731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.	
	Examiner OLEG KORSAK	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Jiang et al. "Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems", IEEE, August 2007
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04Q11/0062, H04L9/0891	5/13/2014	OK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
380	256	5/13/2014	OK
713	163	5/13/2014	OK

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search CPC (H04J3/0655 OR H04N21/6405 ORH04N21/47202 OR H04Q11/0067 ORH04H20/69 OR H04L63/0428 ORH04L63/0435 OR H04L9/08) limited by keywords	2/7/2013	OK
Updated EAST search	5/13/2014	OK
GOOGLE NPL search	5/13/2014	OK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/OLEG KORSAK/ Examiner.Art Unit 2492	
---	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	05/21/2014		
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			EXAMINER KORSAK, OLEG	
			ART UNIT 2492	PAPER NUMBER
			MAIL DATE 05/21/2014	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/257,731	Applicant(s) ZHANG ET AL.	
	Examiner OLEG KORSAK	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08/12/2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1-13 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-13 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) ☒ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____. | 4) ☐ Other: ____. |

DETAILED ACTION

A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 12, 2013 has been entered.

Claims 1, 2 and 7 have been amended. No new claims have been added. Claims 1-13 are currently pending and directed toward a METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM.

Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Arguments

Applicant's arguments with respect to claims 1-13 have been considered but are moot because of new grounds used in the current rejection.

Claim Rejections - 35 USC § 103

Claims 1, 2, 4-7, 9, 10, 12, 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of

Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), hereinafter referred to as He and Jiang2007 respectively.

As per **claim 1**, He teaches a method for encrypting multicast service in a passive optical network system (*a passive optical network pon technology, He, page 2*), the method comprising: an optical line terminal (OLT) generating a common key (*means of generating a key at the optical network line terminal, He, ABSTRACT*), and using the common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in the same one bearer channel use a same common key to carry out encryption (*said key is used as the common key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT*); and said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data (*while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream. He, ABSTRACT*).

He does **not** teach all multicast services, Jiang2007, however teaches using the common key to encrypt multicast service data of all multicast services in a bearer channel (Note that all BS in the same MBS zone use the same key for encrypting the same MBS program. Jiang2007, page 82).

He in view of Jiang2007 are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang2007. This would have been desirable to reduce substantially the handoff delay between BS in the same MBS zone. [Jiang2007, p.82].

As per **claim 2**, He in view of Jiang2007 teaches the method of claim 1, further comprising: after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel (*And the key by using the other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal using the key to multicast data stream decoding receives the multicast data stream. He, Page 3*).

As per **claim 4**, He in view of Jiang2007 teaches the method of claim 1, wherein: the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises: the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU (*Can firstly the optical network user end of the optical network line terminal sends multicast application of optical network line road terminal to the multicast request processing according to user authority is determined whether to the optical network user end distributing multicast. If the user does not multicast authority optical network line terminal is not the multicast request. He, Page 3*).

As per **claim 5**, He in view of Jiang2007 teaches the method of claim 1, wherein: the multicast service data in different bearer channels use different common keys or the same common key (*By using this invention using the same service channels as same as the port id or*

vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6).

As per **claim 6**, He in view of Jiang2007 teaches the method of claim 1, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key (*and the distribution of the multicast occupies a downlink service channel by channel number port id virtual channel identifier vpi or virtual channel identifier address to identify vci port is id. He, Page 5).*

As per **claim 12**, He in view of Jiang2007 teaches the method of claim 2, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key (*the same service channels as same as the port id or vpi/vci of Service channel for the same multicast user transmitting multicast encrypted data streams. He, Page 6).*

Apparatus **claims 7, 9, 10, 13** are drawn to the apparatus corresponding to the method of using the same as claimed in claims 1, 2, 4-6, 12. Therefore apparatus claims 7, 9, 10, 13 correspond to method claims 1, 2, 4-6, 12, and are rejected for the same reasons of obviousness as used above.

Claims 3, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast

Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), further in view of Jiang (CN 1866857 November 22 2006, translation by Dialog), hereinafter referred to as He, Jiang2007 and Jiang2006 respectively.

As per **claims 3 and 8**, He in view of Jiang2007 does not teach the aging time, Jiang2006, however, teaches the method of claim 1 further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (*that receiver the user, OLT distributed of downlink service channel and a common key for user ONT, and timing updating the common downlink service channel and a common key, Jiang2006, ABSTRACT*).

He in view of Jiang2007 in view of Jiang2006 are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He in view of Jiang2007 with the step of Jiang2006. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang2006, p.4].

As per **claim 11**, He in view of Jiang2007 does not teach the aging time, Jiang2006 however teaches the method of claim 2, further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (Steps: 14 OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, and starting timing, wherein the output of downlink service channel and a key, overtime. The gaining the

group multicast data stream of the user request, OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, a OLT generating the novel of downlink service channel number and a starting timing. Jiang2006, Page 4).

He in view of Jiang2007 in view of Jiang2006 are analogous art, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He in view of Jiang2007 with the step of Jiang2006. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang2006, p.4].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSACK whose telephone number is (571)270-1938. The examiner can normally be reached on Monday-Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2492

/O. K./

Examiner, Art Unit 2492

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1011	(380/256 OR 713/163).OCLS.	US-PGPUB; USPAT	OR	OFF	2014/05/13 17:01
L2	3458	(H04Q11/0062 OR H04L9/0891).CPC.	US-PGPUB; USPAT	OR	OFF	2014/05/13 17:02
L3	103	L1 AND L2	US-PGPUB; USPAT	OR	OFF	2014/05/13 17:02
L4	2319	bearer channel	US-PGPUB; USPAT	ADJ	OFF	2014/05/13 17:03
L5	1	L3 AND L4	US-PGPUB; USPAT	ADJ	OFF	2014/05/13 17:03
L6	26425	("same" OR common) key	US-PGPUB; USPAT	ADJ	OFF	2014/05/13 17:05
L7	23	L4 AND L6	US-PGPUB; USPAT	OR	OFF	2014/05/13 17:05
L8	2	L7 AND multicast\$4	US-PGPUB; USPAT	OR	OFF	2014/05/13 17:06
S1	4909	passive optical network	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
S2	790	S1 AND key	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
S3	323	S2 AND encrypt\$3	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:18
S4	101	S3 AND (optical line terminal)	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:19
S5	30	S4 AND multicast	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:19
S6	30	S5 AND tim\$4	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:20
S7	10	S6 AND downlink	US-PGPUB; USPAT	ADJ	OFF	2013/02/07 07:21
S8	16943	((H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR	US-PGPUB;	ADJ	OFF	2013/02/07 07:24

		H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08).CPC.)	USPAT			
S9	1130	S8 AND S1	US- PGPUB; USPAT	ADJ	OFF	2013/02/07 07:25
S10	14	S8 AND S6	US- PGPUB; USPAT	ADJ	OFF	2013/02/07 07:25

EAST Search History (Interference)

< This search history is empty >

5/ 13/ 2014 5:07:50 PM
C:\ Users\ okorsak\ Documents\ e-Red Folder\ 13257731 Zhang\ 13257731 Zhang.wsp

<i>Index of Claims</i> 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	02/07/2013	06/05/2013	05/13/2014					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					

REMARKS

The final Office Action dated May 21, 2014 is carefully reviewed and the following remarks are responsive thereto.

No new matter is added.

Claims 1-13 remain pending. Reconsideration and allowance are respectfully requested.

Claim Rejections - 35 USC § 103

The Office Action rejected claims 1, 2, 4-7, 9, 10, 12, 13 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), hereinafter referred to as He and Jiang2007 respectively.

The Office Action rejected claims 3, 8 and 11 under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), further in view of Jiang (CN 1866857 November 22, 2006, translation by Dialog), hereinafter referred to as He, Jiang2007 and Jiang2006 respectively.

The Applicants respectfully traverse the rejections based on the following remarks.

Claim 1

He alone, or in any proper combination with Jiang, fails to disclose, suggest, or render obvious all of the limitations of claim 1. More particularly, the independent claim 1 recites:

“A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a common key, and **using the common key to encrypt multicast service data of all multicast services in a bearer channel** and then sending encrypted data, wherein **the multicast service data of all multicast services in the same one bearer channel use a same common key** to carry out encryption; and

said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.”

As stated in the previous response to the Office Action, one skilled in the art would know that **one** bearer channel can include **a plurality of** service channels to bear **different** multicast services for different terminals, i.e., one bearer channel may include 3 service channels A, B and C, for example, the service channel A can bear multicast service **1** to terminal a, b and c, the service channel B can bear multicast service **2** to terminal a and c, and the service channel C can bear multicast service **3** to terminal b and c.

In the amended claim 1, the OLT uses **only one** common key to encrypt multicast service data of **all** multicast services which are born in **different** service channels in the same one bearer channel, so that, different ONUs which are legal for the OLT can decrypt the multicast services using the same common key.

In contrast, He discloses to encrypt the multicast data stream in **one** service channel (Abstract, step A3 on page 3, lines 23-24 on page 4, step 4-2) on page 5, etc.), that is, different multicast services should be encrypted by different keys.

Referring the remarks by Applicants in the previous response, and as acknowledged by the Examiner in this office action, He **fails to** disclose the feature “**using the common key to encrypt multicast service data of all multicast services in a bearer channel ...**, wherein **the multicast service data of all multicast services in the same one bearer channel use a same common key** to carry out encryption” in claim 1.

In this Office Action, the Examiner indicated that “He does not teach all multicast services, Jiang2007, however teaches using the common key to encrypt multicast service data of all multicast services in a bearer channel”.

Applicants respectfully disagree.

Jiang2007 discloses:

MBS Zone Management – The MBSC delivers an **MBS program** to one or more MBS zones, each of which **consists of multiple BS of a WiMAX network**. ...Note that all BS in the same MBS zone use the same key **for encrypting the same MBS program**. This reduces substantially the handoff delay between BS in the same MBS zone. (page 82, the last 5 lines in col. 1 and the first 6 lines in col. 2).

Security – ...MBSC is responsible for creating, maintaining, and distributing **a key for each MBS program in each zone**. (page 82, the 3rd paragraph in col. 2).

From the above quotes, it shows that for the **same** MBS program of **ONE** MBS zone, the **same** key for encrypting is used, and the purpose is when the handoff occurs between different BSs in the **ONE** MBS zone, the delay due to the different keys handoff can be avoided. The skilled in the art would know that the handoff between **the different BSs and one MS should be on different bearer channels**. Thus, the same key in Jiang2007 is **not** for “**the multicast service data of all different multicast services in the same one bearer channel**”, **but** is used in the **same** MBS program on different bearer channels between the different BSs and the one MS. Further, Jiang2007 discloses the **MBS services in the WiMAX network** which has **totally different structure** from the PON system.

Therefore, Jiang2007 fails to disclose the feature “**using the common key to encrypt multicast service data of all multicast services in a bearer channel ...**, wherein **the multicast service data of all multicast services in the same one bearer channel use a same common key** to carry out encryption” in claim 1 also.

Further, it is **non-obvious** to a person of ordinary skill in the art to modify He with the step of Jiang2007 because they relate to totally different network systems (PON system and the WiMAX network) respectively and have different networking structures; and further, even though He and Jiang2007 can be combined together, they only teach that **one key for one MBS program**.

In light of the above, He alone, or in any proper combination with Jiang2007, fails to disclose, suggest, or render obvious all of the limitations of claim 1. Thus, for at least the reasons articulated above, claim 1 is allowable over He alone, or in any proper combination with Jiang2007. Applicant respectfully request that this rejection to claim 1 be withdrawn.

Claim 7

Claim 7 defines a device for encrypting multicast service in a passive optical network system corresponding to claim 1.

In light of above, claim 7 is allowable over He alone, or in any proper combination with Jiang2007, for at least the same reasons as claim 1 and more specifically for the specific features it recites.

Claims 2, 4-6, 9, 10, 12, 13

In light of above, claims 2, 4-6, 9, 10, 12, 13 are allowable over He alone, or in any proper combinations with Jiang2007, for at least the same reasons as claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

Claims 3, 8 and 11

In light of above, claims 3, 8 and 11 are allowable over He alone, or in any proper combinations with Jiang2006, for at least the same reasons as claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

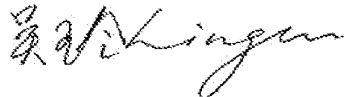
Conclusion

The Applicants believe they have responded to each matter raised by the Examiner. Allowance of the claims is respectfully solicited. It is believed that the present patent application, after the above amendments and statement of opinions, has overcome all the defects pointed out by the Examiner and is in conformity with the relevant provisions, so it should be granted patent rights.

The Applicants expect early granting of patent right for this application. If there is still a problem that the Examiner believes is not overcome by the statement of opinions, please give the Applicants another chance to make amendments and further clarification or explanation or observation.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below. Favorable action is respectfully requested.

Respectfully submitted,

By: _____

Ling Wu

Patent Agent for Applicant

Registration No. 66,304

Date: August 1, 2014
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854
(301) 301-637-2202
(301) 251-0237 (fax)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dezhi Zhang et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **2492**

) Examiner: **KORSAK, OLEG**

Amendments and Response to Non-Final Office Action

Dear Sir / Madam,

Responsive to the non-final Office Action dated May 21, 2014, Applicants submit the following remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable. Favorable reconsideration of the application and withdrawal of the rejections is respectfully requested.

Remarks begins on page 2 of this paper.

Conclusion begins on page 6 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	19753550
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	01-AUG-2014
Filing Date:	20-SEP-2011
Time Stamp:	14:30:19
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Response_to_RCE_1OA_AFD111101435-US_Final.pdf	166586 9b9718b4fce74b0bd21ffb69030672f3b29aa17	no	6

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Search Notes 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04Q11/0062, H04L9/0891	5/13/2014	OK
H04Q11/0062, H04Q2011/0088, H04L9/0891	9/8/2014	OK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
380	256	5/13/2014	OK
713	163	5/13/2014	OK
380	256	9/8/2014	OK
713	163	9/8/2014	OK

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search CPC (H04J3/0655 OR H04N21/6405 ORH04N21/47202 OR H04Q11/0067 ORH04H20/69 OR H04L63/0428 ORH04L63/0435 OR H04L9/08) limited by keywords	2/7/2013	OK
Updated EAST search	5/13/2014	OK
GOOGLE NPL search	5/13/2014	OK
Updated EAST search	9/8/2014	OK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/OLEG KORSAK/ Examiner.Art Unit 2492	
---	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	09/16/2014		
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			EXAMINER KORSAK, OLEG	
			ART UNIT 2492	PAPER NUMBER
			MAIL DATE 09/16/2014	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/257,731	Applicant(s) ZHANG ET AL.	
	Examiner OLEG KORSAK	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08/01/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1-13 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-13 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) ☐ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____. | 4) ☐ Other: ____. |

DETAILED ACTION

Response to Amendment

This action is in response to amendment filed August 01, 2014 for the application # 13/257,731 filed on September 20, 2011.

Claims 1-13 are currently pending and directed toward a METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM.

Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

Claims 1, 2, 4-7, 9, 10, 12, 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), hereinafter referred to as He and Jiang2007 respectively.

As per **claim 1**, He teaches a method for encrypting multicast service in a passive optical network system (*a passive optical network pon technology, He, page 2*), the method comprising: an optical line terminal (OLT) generating a common key (*means of generating a key at the optical network line terminal, He, ABSTRACT*), and using the common key to encrypt multicast

Art Unit: 2492

service data in a bearer channel and then sending encrypted data, the multicast service data in the same one bearer channel use a same common key to carry out encryption (*said key is used as the common key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT*); and said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data (*while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream. He, ABSTRACT*).

He does **not** teach all multicast services, Jiang2007, however teaches using the common key to encrypt multicast service data of all multicast services in a bearer channel (Note that all BS in the same MBS zone use the same key for encrypting the same MBS program. Jiang2007, page 82).

He in view of Jiang2007 are analogous art to claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He with the step of Jiang2007. This would have been desirable to reduce substantially the handoff delay between BS in the same MBS zone. [Jiang2007, p.82].

As per **claim 2**, He in view of Jiang2007 teaches the method of claim 1, further comprising: after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel (*And the key by using the other service channel and sends it to has the group broadcast receiving the authority for user terminal of optical network optical network user terminal using the key to multicast data stream decoding receives the multicast data stream. He, Page 3*).

As per **claim 4**, He in view of Jiang2007 teaches the method of claim 1, wherein: the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises: the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU (*Can firstly the optical network user end of the optical network line terminal sends multicast application of optical network line road terminal to the multicast request processing according to user authority is determined whether to the optical network user end distributing multicast. If the user does not multicast authority optical network line terminal is not the multicast request. He, Page 3*).

As per **claim 5**, He in view of Jiang2007 teaches the method of claim 1, wherein: the multicast service data in different bearer channels use different common keys or the same common key (*By using this invention using the same service channels as same as the port id or vpi/vci of service channel for the same multicast user transmitting multicast encrypted data streams using different service channel are respectively for the same multicast of different user transmitting multicast encrypted key. He, Page 6*).

As per **claim 6**, He in view of Jiang2007 teaches the method of claim 1, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel

identification of the bearer channel where all multicast service data are encrypted with the common key (*and the distribution of the multicast occupies a downlink service channel by channel number port id virtual channel identifier vpi or virtual channel identifier address to identify vci port is id. He, Page 5*).

As per **claim 12**, He in view of Jiang2007 teaches the method of claim 2, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key (*the same service channels as same as the port id or vpi/vci of Service channel for the same multicast user transmitting multicast encrypted data streams. He, Page 6*).

Apparatus **claims 7, 9, 10, 13** are drawn to the apparatus corresponding to the method of using the same as claimed in claims 1, 2, 4-6, 12. Therefore apparatus claims 7, 9, 10, 13 correspond to method claims 1, 2, 4-6, 12, and are rejected for the same reasons of obviousness as used above.

Claims 3, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), further in view of Jiang (CN 1866857 November 22 2006, translation by Dialog), hereinafter referred to as He, Jiang2007 and Jiang2006 respectively.

As per **claims 3 and 8**, He in view of Jiang2007 does not teach the aging time, Jiang2006, however, teaches the method of claim 1 further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it

Art Unit: 2492

regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (*that receiver the user, OLT distributed of downlink service channel and a common key for user ONT, and timing updating the common downlink service channel and a common key, Jiang2006, ABSTRACT*).

He in view of Jiang2007 in view of Jiang2006 are analogous art to claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He in view of Jiang2007 with the step of Jiang2006. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang2006, p.4].

As per **claim 11**, He in view of Jiang2007 does not teach the aging time, Jiang2006 however teaches the method of claim 2, further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data (Steps: 14 OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, and starting timing, wherein the output of downlink service channel and a key, overtime. The gaining the group multicast data stream of the user request, OLT of the group multicast data stream assigns a new of downlink service channel number and new common key, a OLT generating the novel of downlink service channel number and a starting timing. Jiang2006, Page 4).

He in view of Jiang2007 in view of Jiang2006 are analogous art to claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify He in view of

Jiang2007 with the step of Jiang2006. This would have been desirable to achieve the scheduled time for updating the common downlink service channel and respectively each key time [Jiang2006, p.4].

Response to Arguments

Applicant's arguments with regards to claims 1-13 have been fully considered, but they are not persuasive.

“one key for one MBS program” argument – Applicant argues that it is non-obvious to a person of ordinary skill in the art to modify He with the step of Jiang2007 because they relate to totally different network systems (PON system and the WiMAX network) respectively and have different networking structures; and further, even though He and Jiang2007 can be combined together, they only teach that one key for one MBS program (REMARKS, page 4).

Response – Applicant for support of the main argument provided several different arguments, some of each contradict each other. So Examiner has to consider and respond to each of them and additionally all together. First Applicant claims that the skilled in the art would know that the handoff between the different BSs and one MS should be on different bearer channels. At the same time in the same paragraph applicant states that Jiang2007 discloses the MBS services in the WiMAX network which has totally different structure from the PON system (REMARKS, page 4). Although it seems like contradiction, because how POSITA can judge about different bearer channels in Jiang2007 if this it totally different structure than claimed invention?

Examiner actually agrees with Applicant that WiMAX and PON have different structures, the disagreement is: Are those differences important or relevant to make it non obvious for POSITA to combine He and Jiang2007? To answer this question Examiner relies on Applicant's explanation of bearer channel, provided in response: “one skilled in the art would know that one bearer channel can include a plurality of service channels to bear different multicast services for

different terminals, i.e., one bearer channel may include 3 service channels A, Band C, for example, the service channel A can bear multicast service 1 to terminal a, band c, the service channel B can bear multicast service 2 to terminal a and c, and the service channel C can bear multicast service 3 to terminal band c.” (REMARKS, page 3). This can be immediately recognized as description of multicast service. The question arises: Does prior art of Jiang2007 has anything to do with delivering multicast services? And the answer is definitely YES, starting with the title “Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems”, through the purpose of the article “we propose a multicast and broadcast service (MBS) architecture for WiMAX that is based on MBMS. Moreover, we enhance the MBS architecture for mobile WiMAX to overcome the shortcoming of limited video broadcast performance over the baseline MBS model” (Jian2007, ABSTRACT) and up to results “The versatility of mobile WiMAX radio access network (RAN) and all-IP network architecture combined with high throughput, spectral efficiency, and data rates (if compared with 3GPP systems) have made mobile WiMAX one of the most viable radio access technologies to deliver a variety of unicast, broadcast, and multicast services and applications, including voice over IP (VoIP) and mobile TV.” (Jian2007, CONCLUSION). It follows that Jiang2007 applies general principles of multicasting to a specific transport infrastructure which happens to be WiMAX to overcome the shortcoming of degraded video broadcast performance over the baseline MBS model. Therefore it is OBVIOUS to apply the approach and proposed solutions to other technologies used to deliver a variety of unicast, broadcast, and multicast services such as PON systems.

Further, Examiner puts on record that, as applicable in context of claimed invention, MBS zone of Jiang2007 is equivalent to bearer channel of Applicant. Therefore limitation “the multicast

service data of all multicast services in the same one bearer channel use a same common key” is equivalent to “all BS in the same MBS zone use the same key for encrypting the same MBS program”. It should be also noted that limitation using the common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in the same one bearer channel use a same common key to carry out encryption (said key is used as the common key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT). It follows that cited limitations of Claim 1 are obvious over HE in view of Jiang2007.

Applicant made a valid argument that Jiang2007 teaches the common key for all BS encrypting the same MBS program (REMARKS, page 4). It follows that although the key is common for all BS it may be different for different time when another MBS program is delivered. However, it is similar to limitation “setting an aging time for the common key” of current claims 3 and 8, where aging time may be set to duration of the MBS program. It should be also noted that Jian2007 has no teachings that the common key SHOULD be different for each MBS program, considering this as a choice. Therefore limitations of claim 1 are obvious over He in view of Jiang 2007 and Examiner maintains rejections.

Conclusion -Therefore, in view of the above reasons, Examiner maintains rejections.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSACK whose telephone number is (571)270-1938. The examiner can normally be reached on Monday-Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 13/257,731
Art Unit: 2492

Page 11

/Zachary A Davis/
Primary Examiner, Art Unit 2492

/O. K./

Examiner, Art Unit 2492

<i>Index of Claims</i> 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	02/07/2013	06/05/2013	05/13/2014	09/08/2014				
	1	✓	✓	✓	✓				
	2	✓	✓	✓	✓				
	3	✓	✓	✓	✓				
	4	✓	✓	✓	✓				
	5	✓	✓	✓	✓				
	6	✓	✓	✓	✓				
	7	✓	✓	✓	✓				
	8	✓	✓	✓	✓				
	9	✓	✓	✓	✓				
	10	✓	✓	✓	✓				
	11	✓	✓	✓	✓				
	12	✓	✓	✓	✓				
	13	✓	✓	✓	✓				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3944	(H04Q11/0062, H04Q2011/0088, H04L9/0891).cpc.	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:03
L2	11143	((passive optical network) OR PON)	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L3	6310	passive optical network	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L4	1045	L3 AND key	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L5	428	L4 AND encrypt\$3	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L6	140	L5 AND (optical line terminal)	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L7	42	L6 AND multicast	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L8	42	L7 AND tim\$4	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L9	12	L8 AND downlink	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L10	18900	((H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08).CPC.)	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L11	1640	L10 AND L3	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L12	25	L10 AND L8	US-PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L13	1036	(380/256 OR 713/163).OCLS.	US-PGPUB; USPAT	OR	OFF	2014/09/08 08:05
L14	3633	(H04Q11/0062 OR H04L9/0891).CPC.	US-PGPUB; USPAT	OR	OFF	2014/09/08 08:05
L15	113	L13 AND L14	US-PGPUB; USPAT	OR	OFF	2014/09/08 08:05
L16	2373	bearer channel	US-	ADJ	OFF	2014/09/08

			PGPUB; USPAT			08:05
L17	1	L15 AND L16	US- PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L18	27297	("same" OR common) key	US- PGPUB; USPAT	ADJ	OFF	2014/09/08 08:05
L19	23	L16 AND L18	US- PGPUB; USPAT	OR	OFF	2014/09/08 08:05
L20	2	L19 AND multicast\$4	US- PGPUB; USPAT	OR	OFF	2014/09/08 08:05
L21	119	L1 AND L13	US- PGPUB; USPAT	OR	OFF	2014/09/08 08:06
L22	16	L21 AND L2	US- PGPUB; USPAT	OR	OFF	2014/09/08 08:06
L23	10	L22 AND multicast\$4	US- PGPUB; USPAT	ADJ	OFF	2014/09/08 08:06
L24	1	L23 AND L16	US- PGPUB; USPAT	ADJ	OFF	2014/09/08 08:07

EAST Search History (Interference)

< This search history is empty >

9/ 8/ 2014 8:07:43 AM

C:\ Users\ okorsak\ Documents\ e-Red Folder\ 13\ 13257731 Zhang\ 13257731 Zhang.wsp

Electronic Acknowledgement Receipt

EFS ID:	20661730
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	Method and Device for Encrypting Multicast Service in Passive Optical Network System
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	11-NOV-2014
Filing Date:	20-SEP-2011
Time Stamp:	12:59:58
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	AFD111101435-US_Response_to_RCE_FOA_Final.pdf	200494 a037995c7c16ef0136d4be6d009108bfb2555a5b	no	10

Warnings:

Information:

2	After Final Consideration Program Request	AFCP20_sb0434_AFD111101435-US.pdf	227707 137c72527e31c3bf57017cf0fa4292e489d71ea7	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				428201	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0		
Practitioner Docket No.: AFD111101435-US	Application No.: 13/257,731	Filing Date: 09/20/2011
First Named Inventor: Dezhi Zhang	Title: Method and Device for Encrypting Multicast Service in Passive Optical Network System	
<p>APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.</p> <ol style="list-style-type: none"> 1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (<i>e.g.</i>, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c). 2. The above-identified application contains an outstanding final rejection. 3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect. 4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection. 5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response. 6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web). 7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.] 8. By filing this certification and request, applicant acknowledges the following: <ul style="list-style-type: none"> • Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0. • The examiner will verify that the AFCP 2.0 submission is compliant, <i>i.e.</i>, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions: <ul style="list-style-type: none"> ○ The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, by mailing an advisory action. ○ If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview. <ul style="list-style-type: none"> ▪ The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate. ▪ If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116. 		
Signature /Ling Wu/	Date 11/11/2014	
Name (Print/Typed) Ling Wu	Practitioner Registration No. 66304	
<p>Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.</p>		
☐ * Total of _____ forms are submitted.		

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

REMARKS

The final Office Action dated September 16, 2014 is carefully reviewed and the following amendments and remarks are responsive thereto.

Claims 1 and 7 are amended. No new matter is added.

Claims 1-13 remain pending. Reconsideration and allowance are respectfully requested.

Claim Rejections - 35 USC § 103

The Office Action rejected claims 1, 2, 4-7, 9, 10, 12, 13 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), hereinafter referred to as He and Jiang2007 respectively.

The Office Action rejected claims 3, 8 and 11 under 35 U.S.C. 103(a) as being unpatentable over He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007), further in view of Jiang (CN 1866857 November 22, 2006, translation by Dialog), hereinafter referred to as He, Jiang2007 and Jiang2006 respectively.

The Applicants respectfully traverse the rejections based on the above amendment and the following remarks.

Claim 1

He alone, or in any proper combination with Jiang2007, fails to disclose, suggest, or render obvious all of the limitations of the amended claim 1. More particularly, the amended claim 1 recites:

“A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a common key, and **using the common key to encrypt multicast service data of all different multicast services in a same bearer channel** and then sending encrypted data, wherein **the multicast service data of**

all different multicast services in the same one bearer channel use a same common key to carry out encryption; and

said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.” (Emphasis is added with bold)

As stated in the previous response to the Office Action, One skilled in the art would know that: 1) **one bearer channel** can include a plurality of service channels to **bear different multicast services for different terminals**, and 2) bearer channels between **the different BSs** and one MS **should be different**.

In the amended claim 1, the OLT uses **only one** common key to encrypt multicast service data of **all different** multicast services which are born in **different** service channels in the **same** one bearer channel, so that, different ONUs which are legal for the OLT can decrypt the multicast services using the same common key.

Thus, based on the remarks by Applicants in the previous responses and the Examiner’s admission, He **fails to** disclose the feature “**using the common key to encrypt multicast service data of all multicast services in a bearer channel**” of claim 1.

However, in this Office Action, the Examiner maintain the opinion that “He does not teach all multicast services, Jiang2007, however teaches using the common key to encrypt multicast service data of all multicast services in a bearer channel”.

Responsive to the above Examiner’s opinion, Applicants further amend this feature of claim 1 and respectfully submit that the feature “using the common key to encrypt multicast service data of all different multicast services in a same bearer channel ... wherein the multicast service data of all different multicast services in the same one bearer channel use a same common key to carry out encryption” in the amended claim 1 is **not** disclosed by Jiang2007.

In page 9 of the Office Action, the Examiner indicated that “Applicant made a valid argument that Jiang2007 teaches the common key for all BSs encrypting the same MBS program. *It follows that although the key is common for all BS it may be different for different time when another MBS program is delivered.* ...It should be also noted that Jiang2007 has no

teachings that the common key SHOULD be different for each MBS program, considering this as a choice.”

Per the Examiner’s understanding, *the key may be **same** for different time when another MBS program is delivered*. However, the Applicants interpret that whether the keys are same or different for different MBS program **is irrelevant** to the time, it is **an additional choice** of whether to update the key according to an aging time.

From the disclosure of Jiang2007, it can **only** be seen that **Jiang2007 teaches the common key for all BSs encrypting the same MBS program**. It is a common knowledge of a person skilled in the art that different BSs carry the same MBS program on different bearer channels. A person skilled in the art, combining Jiang2007 with the common knowledge, can only acquire a solution that the common key for all different BSs encrypting the **same** MBS program in the **different** bearer channels, which is totally **contrary** to the feature that “using the common key to encrypt multicast service data of all different multicast services in a same bearer channel” defined in the amended claim 1.

Therefore, Jiang2007 fails to disclose the feature “using the common key to encrypt multicast service data of all different multicast services in a same bearer channel ... wherein the multicast service data of all different multicast services in the same one bearer channel use a same common key to carry out encryption” defined in the amended claim 1.

In light of the above, He alone, or in any proper combination with Jiang2007, fails to disclose, suggest, or render obvious all of the limitations of the amended claim 1. Thus, for at least the reasons articulated above, the amended claim 1 is allowable over He alone, or in any proper combination with Jiang2007. Applicant respectfully request that this rejection to claim 1 be withdrawn.

Claim 7

The amended claim 7 defines a device for encrypting multicast service in a passive optical network system corresponding to the amended claim 1.

In light of above, the amended claim 7 is allowable over He alone, or in any proper combination with Jiang2007, for at least the same reasons as the amended claim 1 and more specifically for the specific features it recites.

Claims 2, 4-6, 9, 10, 12, 13

In light of above, claims 2, 4-6, 9, 10, 12, 13 are allowable over He alone, or in any proper combinations with Jiang2007, for at least the same reasons as the amended claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

Claims 3, 8 and 11

In light of above, claims 3, 8 and 11 are allowable over He alone, or in any proper combinations with Jiang2006, for at least the same reasons as the amended claim 1 or 7 from which they depend, and more specifically for the specific features they recite.

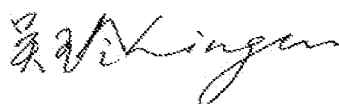
Conclusion

The Applicants believe they have responded to each matter raised by the Examiner. Allowance of the claims is respectfully solicited. It is believed that the present patent application, after the above amendments and statement of opinions, has overcome all the defects pointed out by the Examiner and is in conformity with the relevant provisions, so it should be granted patent rights.

The Applicants expect early granting of patent right for this application. If there is still a problem that the Examiner believes is not overcome by the statement of opinions, please give the Applicants another chance to make amendments and further clarification or explanation or observation.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below. Favorable action is respectfully requested.

Respectfully submitted,


By: _____

Ling Wu

Patent Agent for Applicant

Registration No. 66,304

Date: November 11, 2014
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854
(301) 637-2202 (tel)
(301) 251-0237 (fax)

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for encrypting multicast service in a passive optical network system, the method comprising:

an optical line terminal (OLT) generating a common key, and using the common key to encrypt multicast service data of all different multicast services in a same bearer channel and then sending encrypted data, wherein the multicast service data of all different multicast services in the same one bearer channel use a same common key to carry out encryption; and

said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.

2. (Previously Presented) The method of claim 1, further comprising:

after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel.

3. (Previously Presented) The method of claim 1, further comprising:

said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

4. (Previously Presented) The method of claim 1, wherein:

the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises:

the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or

the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU.

5. (Previously Presented) The method of claim 1, wherein:

the multicast service data in different bearer channels use different common keys or the same common key.

6. (Previously Presented) The method of claim 1, wherein:

in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

7. (Currently Amended) A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein:

said key generation unit is configured to: generate a common key;

said encryption unit is configured to: encrypt multicast service data of all different multicast services born in a same one bearer channel with a same common key;

said sending unit is configured to: send the encrypted multicast service data, and send the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data.

8. (Previously Presented) The device of claim 7, wherein,

said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the common key, and when the aging time arrives, notifying said key generation unit to regenerate a common key.

9. (Previously Presented) The device of claim 7, wherein:

said sending unit is configured to apply following methods to send the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the common key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast service data, and then sending the common key applied in encrypting the multicast service data to the ONU.

10. (Previously Presented) The device of claim 7, wherein,

said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

11. (Previously Presented) The method of claim 2, further comprising:

said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

12. (Previously Presented) The method of claim 2, wherein:

in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

13. (Previously Presented) The device of claim 9, wherein,

said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dezhi Zhang et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **2492**

) Examiner: **KORSAK, OLEG**

)

Amendments and Response to Final Office Action

Dear Sir / Madam,

Responsive to the final Office Action dated September 16, 2014, Applicants submit the following remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable. Favorable reconsideration of the application and withdrawal of the rejections is respectfully requested.

Amendments to the Claims are reflected in the listing of the claims, which begins on page 2 of this paper.

Remarks begins on page 6 of this paper.

Conclusion begins on page 10 of this paper.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/257,731		Filing Date 09/20/2011		☐ To be Mailed	
---	--	--	--	--	---	--	----------------------------------	--	---------------------------------------	--

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

(Column 1)		(Column 2)				(Column 1)		(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)			FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A					
☐ SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A			N/A					
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A					
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*			X \$	=				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*			X \$	=				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))			If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL				

APPLICATION AS AMENDED – PART II

(Column 1)		(Column 2)		(Column 3)				(Column 1)		(Column 2)	
AMENDMENT	11/11/2014	CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)			ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0			X \$80 =			0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0			X \$420 =			0
☐ Application Size Fee (37 CFR 1.16(s))											
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE		0	

(Column 1)		(Column 2)		(Column 3)				(Column 1)		(Column 2)	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)			ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=			X \$	=		
	Independent (37 CFR 1.16(h))	*	Minus	***	=			X \$	=		
☐ Application Size Fee (37 CFR 1.16(s))											
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE			

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/JAMES MASON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

<i>Index of Claims</i> 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47				
CLAIM		DATE								
Final	Original	02/07/2013	06/05/2013	05/13/2014	09/08/2014	11/14/2014				
1	1	✓	✓	✓	✓	=				
2	2	✓	✓	✓	✓	=				
5	3	✓	✓	✓	✓	=				
6	4	✓	✓	✓	✓	=				
7	5	✓	✓	✓	✓	=				
8	6	✓	✓	✓	✓	=				
9	7	✓	✓	✓	✓	=				
10	8	✓	✓	✓	✓	=				
11	9	✓	✓	✓	✓	=				
12	10	✓	✓	✓	✓	=				
3	11	✓	✓	✓	✓	=				
4	12	✓	✓	✓	✓	=				
13	13	✓	✓	✓	✓	=				

Issue Classification 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

CPC						
Symbol					Type	Version
H04Q		11	/	0062	F	2013-01-01
H04L		9	/	0891	I	2013-01-01
H04Q		2011	/	0088	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets					
Symbol		Type	Set	Ranking	Version
					
					

/OLEG KORSAK/ Examiner.Art Unit 2492	11/14/2014	Total Claims Allowed: 13	
(Assistant Examiner)	(Date)		
/SALEH NAJJAR/ Supervisory Patent Examiner.Art Unit 2492	11/14/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

☐ Claims renumbered in the same order as presented by applicant															
☐ CPA															
☐ T.D.															
☐ R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1														
2	2														
5	3														
6	4														
7	5														
8	6														
9	7														
10	8														
11	9														
12	10														
3	11														
4	12														
13	13														

/OLEG KORSAK/ Examiner.Art Unit 2492		11/14/2014		Total Claims Allowed:	
(Assistant Examiner)		(Date)		13	
/SALEH NAJJAR/ Supervisory Patent Examiner.Art Unit 2492		11/14/2014		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)		(Date)		1	1

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	6520	passive optical network	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L8	1089	L7 AND key	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L9	440	L8 AND encrypt\$3	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L10	145	L9 AND (optical line terminal)	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L11	45	L10 AND multicast	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L12	45	L11 AND tim\$4	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L13	12	L12 AND downlink	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L14	19504	((H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08).CPC.)	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L15	1702	L14 AND L7	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L16	26	L14 AND L12	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L17	1054	(380/256 OR 713/163).OCLS.	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L18	3696	(H04Q11/0062 OR H04L9/0891).CPC.	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L19	113	L17 AND L18	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L20	2410	bearer channel	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L21	1	L19 AND L20	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L22	27893	("same" OR common) key	US-	ADJ	OFF	2014/11/14

			PGPUB; USPAT			10:23
L23	23	L20 AND L22	US- PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L24	2	L23 AND multicast\$4	US- PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L25	4013	(H04Q11/0062, H04Q2011/0088, H04L9/0891).cpc.	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L26	11444	((passive optical network) OR PON)	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L27	6520	passive optical network	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L28	1089	L27 AND key	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L29	440	L28 AND encrypt\$3	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L30	145	L29 AND (optical line terminal)	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L31	45	L30 AND multicast	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L32	45	L31 AND tim\$4	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L33	12	L32 AND downlink	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L34	19504	((H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08).CPC.)	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L35	1702	L34 AND L27	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L36	26	L34 AND L32	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L37	1054	(380/256 OR 713/163).CCLS.	US- PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L38	3696	(H04Q11/0062 OR H04L9/0891).CPC.	US- PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L39	113	L37 AND L38	US- PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L40	2410	bearer channel	US- PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23

L41	1	L39 AND L40	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L42	27893	("same" OR common) key	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L43	23	L40 AND L42	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L44	2	L43 AND multicast\$4	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L45	120	L25 AND L37	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L46	17	L45 AND L26	US-PGPUB; USPAT	OR	OFF	2014/11/14 10:23
L47	11	L46 AND multicast\$4	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23
L48	1	L47 AND L40	US-PGPUB; USPAT	ADJ	OFF	2014/11/14 10:23

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	291	(380/256 OR 713/163).CCLS.	US-PGPUB; UPAD	OR	OFF	2014/11/14 10:21
L2	2106	(H04Q11/0062, H04Q2011/0088, H04L9/0891).cpc.	US-PGPUB; UPAD	ADJ	OFF	2014/11/14 10:22
L3	35	L1 AND L2	US-PGPUB; UPAD	ADJ	OFF	2014/11/14 10:22
L4	23	L3 AND multicast\$4	US-PGPUB; UPAD	ADJ	OFF	2014/11/14 10:22
L5	1176	bearer channel	US-PGPUB; UPAD	ADJ	OFF	2014/11/14 10:23
L6	1	L4 AND L5	US-PGPUB; UPAD	ADJ	OFF	2014/11/14 10:23

11/ 14/ 2014 10:25:28 AM
c:\ users\ okorsak\ documents\ e-red folder\ 13\ 13257731 zhang\ 13257731 zhang.wsp

Search Notes 	Application/Control No. 13257731	Applicant(s)/Patent Under Reexamination ZHANG ET AL.
	Examiner OLEG KORSAK	Art Unit 2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04Q11/0062, H04L9/0891	5/13/2014	OK
H04Q11/0062, H04Q2011/0088, H04L9/0891	9/8/2014	OK
H04Q11/0062, H04Q2011/0088, H04L9/0891	11/14/2014	OK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
380	256	5/13/2014	OK
713	163	5/13/2014	OK
380	256	9/8/2014	OK
713	163	9/8/2014	OK
380	256	11/14/2014	OK
713	163	11/14/2014	OK

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search CPC (H04J3/0655 OR H04N21/6405 OR H04N21/47202 OR H04Q11/0067 OR H04H20/69 OR H04L63/0428 OR H04L63/0435 OR H04L9/08) limited by keywords	2/7/2013	OK
Updated EAST search	5/13/2014	OK
GOOGLE NPL search	5/13/2014	OK
Updated EAST search	9/8/2014	OK
Updated EAST search	11/14/2014	OK

INTERFERENCE SEARCH

/OLEG KORSAK/ Examiner.Art Unit 2492	
---	--

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
380	256	11/14/2014	OK
713	163	11/14/2014	OK
H04Q11	0062	11/14/2014	OK
H04Q2011	0088	11/14/2014	OK
H04L9	0891	11/14/2014	OK

/OLEG KORSAK/
Examiner.Art Unit 2492

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dezhi Zhang et al.

Serial No.: **13/257,731**

Filed: **09/20/2011**

For: **Method and Device for Encrypting**

**Multicast Service in Passive Optical Network
System**

) Customer No.: **95957**

) Confirmation No.: **6831**

) Art Unit: **2492**

) Examiner: **KORSAK, OLEG**

)

Amendments and Response to Final Office Action

Dear Sir / Madam,

Responsive to the final Office Action dated September 16, 2014, Applicants submit the following remarks. In light of these amendments and remarks, Applicants respectfully assert that all of the claims of patent application are patentable. Favorable reconsideration of the application and withdrawal of the rejections is respectfully requested.

Amendments to the Claims are reflected in the listing of the claims, which begins on page 2 of this paper.

Remarks begins on page 6 of this paper.

Conclusion begins on page 10 of this paper.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

95957 7590 11/17/2014
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854

EXAMINER

KORSAK, OLEG

ART UNIT

PAPER NUMBER

2492

DATE MAILED: 11/17/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

13/257,731

09/20/2011

Dezhi Zhang

AFD111101435-US

6831

TITLE OF INVENTION: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	02/17/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or **Fax** (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

95957 7590 11/17/2014
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831

TITLE OF INVENTION: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	02/17/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
KORSAK, OLEG	2492	380-256000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831
95957	7590	11/17/2014	EXAMINER	
Ling Wu 1107 Bettstrail Way Potomac, MD 20854			KORSAK, OLEG	
			ART UNIT	PAPER NUMBER
			2492	
DATE MAILED: 11/17/2014				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/257,731	Applicant(s) ZHANG ET AL.	
	Examiner OLEG KORSAK	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11/11/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-13. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☒ All b) ☐ Some *c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date ____	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other ____
--	--

/OLEG KORSAK/ Examiner, Art Unit 2492	
--	--

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This action is in response to amendment filed on 11/11/2014 and After Final Consideration Program Request.

By this amendment, claims 1 and 7 have been amended. No new claims have been added. Thus, claims 1-13 are presented for further consideration.

No new IDS have been submitted.

Response to Arguments

Applicant's arguments regarding the amendment submitted on 11/11/2014 have been considered and are persuasive. Applicant's submitted request for AFCP 2.0 is a proper request and is accepted, because the AFCP 2.0 requirements:

1. Request form (PTO/SB/434);
2. Timely filed according to after final practice;
3. Amendment to at least one Independent Claim without broadening the scope in any aspect, and Statement verifying willingness and availability for an examiner initiated interview have been met. Examiner conducted further search and determined patentability of the amended claims. The rejections under pre-AIA 35 U.S.C. 103(a) have been withdrawn.

Allowable Subject Matter

Claims 1-13 are allowed.

The following is an examiner's statement of reasons for allowance in view of Applicant's remarks in the response filed on November 11, 2014:

although the prior art of record such as He (CN 1855834 November 1, 2006, translation by Dialog) in view of Jiang et al. (Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, August 2007) teaches

a method for encrypting multicast service in a passive optical network system (a passive optical network pon technology, He, page 2), the method comprising: an optical line terminal (OLT) generating a common key (means of generating a key at the optical network line terminal, He, ABSTRACT), and using the common key to encrypt multicast service data in a bearer channel and then sending encrypted data, the multicast service data in the same one bearer channel use a same common key to carry out encryption (said key is used as the common key of the multicast and is used to encrypt the multicast bit-stream, He, ABSTRACT); and said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data (while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream. He, ABSTRACT);

none of the prior art of record alone or in combination teaches using the common key to encrypt multicast service data of all different multicast services in a same bearer channel and then sending encrypted data, wherein the multicast service data of all

Art Unit: 2492

different multicast services in the same one bearer channel use a same common key to carry out encryption.

See also Final Office action (09/16/2014, page 9).

The closest prior art made of record are:

NPL "Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems", by Jiang et al. discloses the MBS architecture for mobile WiMAX to overcome the shortcoming of limited video broadcast performance over the baseline MBS model.

CN Patent No. 1855834 by He discloses generating a key at the optical network line terminal, and said key is used as the public key of the multicast and is used to encrypt the multicast bit-stream while said key is transmits to optical user end having multicast receiving right by using another service channel in order to make user end receive and decrypt the encrypted bit-stream.

CN Patent No. 1866857 by Jiang discloses for the authorized user, OLT distributes common descending business channel number and common key for the ONT and refreshes common descending business channel number and common key.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSAK whose telephone number is (571)270-

Art Unit: 2492

1938. The examiner can normally be reached on Monday-Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/O. K./
Examiner, Art Unit 2492

/Saleh Najjar/
Supervisory Patent Examiner, Art Unit 2492

Electronic Acknowledgement Receipt

EFS ID:	20958791
Application Number:	13257731
International Application Number:	
Confirmation Number:	6831
Title of Invention:	METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM
First Named Inventor/Applicant Name:	Dezhi Zhang
Customer Number:	95957
Filer:	Ling Wu
Filer Authorized By:	
Attorney Docket Number:	AFD111101435-US
Receipt Date:	15-DEC-2014
Filing Date:	20-SEP-2011
Time Stamp:	12:33:23
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 960
RAM confirmation Number	9970
Deposit Account	505648
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

--	--	--	--	--	--

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	PartB_Fees_Transmittal_AFD111101435-US.pdf	603690	no	1
			24d76d2582e1aacdb45a1ae064955defa5b1ab36		

Warnings:**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	32459	no	2
			9a753b6aa0a0fa0302814f9fa31835fac692f39c		

Warnings:**Information:**

Total Files Size (in bytes):			636149
------------------------------	--	--	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal				
Application Number:		13257731		
Filing Date:		20-Sep-2011		
Title of Invention:		METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM		
First Named Inventor/Applicant Name:		Dezhi Zhang		
Filer:		Ling Wu		
Attorney Docket Number:		AFD111101435-US		
Filed as Large Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Utility Appl Issue Fee	1501	1	960	960
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 or **Fax** (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

95957 7590 11/17/2014
 Ling Wu
 1107 Bettstrail Way
 Potomac, MD 20854

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	09/20/2011	Dezhi Zhang	AFD111101435-US	6831

TITLE OF INVENTION: METHOD AND DEVICE FOR ENCRYPTING MULTICAST SERVICE IN PASSIVE OPTICAL NETWORK SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	02/17/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
KORSAK, OLEG	2492	380-256000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.563).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47, Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
 (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Ling Wu
 2. Stephen Yang
 3. Ling and Yang
 Intellectual Property

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

ZTE CORPORATION

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Shenzhen City, Guangdong Province
 P. R. China

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505648 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature

Ling Wu
 Ling Wu

Date

12/15/2014

Typed or printed name

Registration No.

66304

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	13257731
Filing Date	2012-01-06
First Named Inventor	Dezhi Zhang et al.
Art Unit	2492
Examiner Name	KORSAK, OLEG
Attorney Docket Number	AFD111101435-US

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
Change(s) applied to document, /K.D.D./ 12/16/2014	1	20060031936	A1	2006-02-09	Nelson et al. Enterasys Networks, Inc.			
	2	20070133800	A1	2007-06-14	Electronics & Telecommunications Research Institute Kim et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	101547086	CN	A	2009-09-30	HUAWEI TECHNOLOGIES CO., LTD.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/257,731	01/27/2015	8942378	AFD111101435-US	6831

95957 7590 01/07/2015
Ling Wu
1107 Bettstrail Way
Potomac, MD 20854

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 131 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Dezhi Zhang, Shenzhen City, CHINA;
Liquan Yuan, Shenzhen City, CHINA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.