

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US2004/016616

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G07C9/00		
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 7 G07C G07F		
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 practical, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DATABASE WPI Section EI, Derwent Publications Ltd., London, GB; Class T01, AN 2003-145718 XP002299947 "SERIAL COMMUNICATION INTERFACE FOR CONTROLLING ENTRANCE AND EXIT HAVING WIEGAND SIGNAL AUTOMATICALLY GENERATING DEVICE" & KR 2002 073 716 A (SUN SANG GYU) 28 September 2002 (2002-09-28)	1-5
Y	abstract	6-8
Y	US 5 475 378 A (CHARLTON BILL ET AL) 12 December 1995 (1995-12-12)	6-8
A	column 3, line 1 - column 4, line 14 figures	1
----- -/--		
☒ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in 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 document 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 8 October 2004		Date of mailing of the international search report 20/10/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Miltgen, E

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/016616

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, A	US 2003/200446 A1 (CANNON GREG L ET AL) 23 October 2003 (2003-10-23) paragraph '0021! - paragraph '0029! figures	1-8
A	US 5 517 172 A (CHIU MANFRED F) 14 May 1996 (1996-05-14) column 2, line 35 - column 4, line 10 figure 1	1
A	US 2002/174357 A1 (DAVIS MICHAEL ET AL) 21 November 2002 (2002-11-21)	

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/016616

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
KR 2002073716	A	28-09-2002	NONE	
US 5475378	A	12-12-1995	CA 2098973 A1	23-12-1994
US 2003200446	A1	23-10-2003	WO 03090403 A1	30-10-2003
US 5517172	A	14-05-1996	NONE	
US 2002174357	A1	21-11-2002	CA 2443086 A1	17-10-2002
			EP 1374157 A1	02-01-2004
			WO 02082367 A1	17-10-2002

Form PCT/ISA/210 (patent family annex) (January 2004)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 November 2006 (23.11.2006)

PCT

(10) International Publication Number
WO 2006/123316 A2

(51) International Patent Classification: **Not classified**

(21) International Application Number:
PCT/IB2006/051593

(22) International Filing Date: 19 May 2006 (19.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05104296.8 20 May 2005 (20.05.2005) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GRAEBER, Frank** [DE/DE]; C/o Triester Strasse 64, A-1101 Vienna (AT).
TOBERGTE, Wolfgang [DE/DE]; C/o Triester Strasse 64, A-1101 Vienna (AT).

(74) Agents: **RÖGGLA, Harald** et al.; Philips Intellectual Property & Standards, Triester Strasse 64, A-1101 Vienna (AT).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

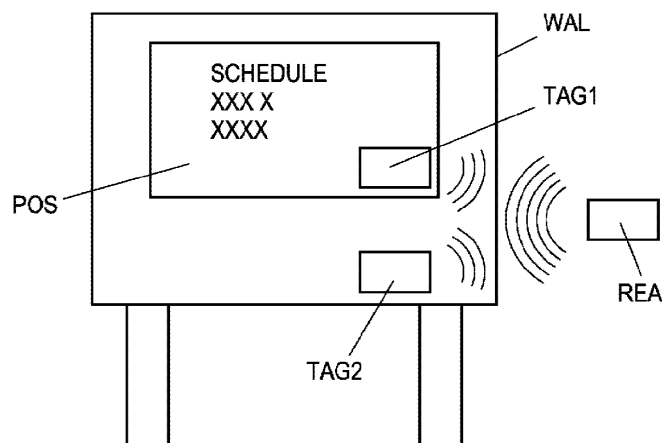
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF SECURELY READING DATA FROM A TRANSPONDER



(57) Abstract: The invention discloses a method of reading data (dat) from a first transponder (TAG1) into a transceiver (REA). Said (dat) are only transmitted from the first transponder (TAG1) to the transceiver (REA) when a second transponder (TAG2) is present within the RFID communication range of the transceiver (REA) and if a positive authentication procedure between the two transponders (TAG1, TAG2) within the RFID communication range of the transceiver (REA) takes place. The second transponder (TAG2) is preferably a stationary transponder (TAG2), whereas the first transponder (TAG1) may be a mobile transponder. The invention further relates to transponders (TAG1, TAG2) as well as to a transceiver (REA) used in such a method of reading data (dat). Furthermore, the invention relates to a poster (POS), to which a first transponder (TAG1) is attached, and to a poster wall (WAL) for attaching such a poster (POS) and a second transponder (TAG2).

WO 2006/123316 A2

Method of securely reading data from a transponder

FIELD OF THE INVENTION

The invention relates to a method of reading data from a first transponder into a transceiver, a transponder for communication with a further transponder via a transceiver, a transceiver for controlling the communication of two transponders, a poster equipped with a transponder, and a poster wall equipped with a poster and a transponder.

BACKGROUND OF THE INVENTION

Identification products such as smart cards and RFID ("Radio Frequency Identification") tags (hereinafter referred to as "transponder") are widely used in the field of transport (ticketing, road tolling, baggage tagging), finance (debit and credit cards, electronic purse, merchant card), communication (SIM cards for GSM phones), and tracking (access control, inventory management, asset tracking). International standard ISO14443A is an industry standard for contactless smart cards. ISO14443A-compliant products such as MIFARE™ provide RF communication technology for transmitting data between a card or a tag and a reader device (hereinafter referred to as "transceiver"). For example, in electronic ticketing for public transport, travelers just wave their card over a reader at the turnstiles or entry point, benefiting from improved convenience and speed in the ticketing process. Such products are set to be the key to individual mobility in the future, supporting multiple applications including road tolling, airline tickets, access control and many more.

Evolving from a combination of contactless identification and networking technologies, Near Field Communication (NFC) is a very short-range wireless technology for distances measured in centimeters, and is optimized for intuitive, easy and secure communication between various devices without user configuration. In order to make two devices communicate, users bring them close together or even make them touch each other. The NFC interfaces of these devices will automatically connect and configure themselves to form a peer-to-peer network. NFC can also bootstrap other protocols like Bluetooth™ or Wireless Ethernet (WiFi) by exchanging the configuration and session data. NFC is compatible with contactless smart card platforms. This enables NFC devices to read information from these cards, making contactless smart cards the ideal solution for bringing

information and vouchers into the NFC world. NFC interfaces are nowadays widely used in mobile phones and other mobile devices.

For example, "smart posters" are known as arbitrary or advertising poster placards, which are equipped with a transponder, such as a passive RFID tag. The data stored
5 on the transponder can be read by using a transceiver, which may be embodied as a traditional smart card reader/writer or as an NFC-enabled mobile device such as a mobile phone.

The data may be stored directly on the transponder or - in a typical smart poster application - the „data“ are stored in the form of a URL (“Uniform Resource Locator”)
10 on the transponder, which URL represents a link or a reference to a designated service, resource or to the „real“ data. By touching the smart poster with the transceiver, the phone automatically establishes a connection (for example, a GPRS connection) to a remote web server and loads the content/data as referenced by the URL to the transceiver.

Specific solutions sometimes make it necessary that a transponder, such as the
15 above-mentioned RFID tag or a contactless smart card, only works at a specific position/location or in a specific, defined region. Especially a smart poster as mentioned above will only work at specific, designated locations, and must not work anywhere else. For example, if a transponder (or the corresponding smart poster) is used in a public transportation system for a check-in into this system, a user has to „touch“ a smart poster to
20 check in. Using this procedure, the user „buys“ a ticket for the public transportation system.

For such an application, it is mandatory that the check-in process only works at the specific location where the smart poster has been installed by the public transport operator. If this requirement were not realized, a malicious user could remove the smart poster with the transponder for the check-in (or the transponder from the poster), then enter
25 the public transportation system, and if he recognized a conductor, he could check in by touching the stolen smart poster or the stolen smart poster transponder. In such a situation, it must be guaranteed that the smart poster or the smart poster transponder must not work if it has been removed from its designated location, and it must be guaranteed that the check-in process is bound to the designated location.

30 In another example, in which it is necessary that a transponder (on, for example, a poster) only works at a specific location, the operator of said transponder, which may have stored certain information for different consumers, etc., is interested in measuring and evaluating the number and/or the frequency of touches to a certain transponder at a specific location, so that the operator can identify attractive locations for installing such

transponders/posters. Here, the functionality of the smart poster tags must also be location-dependent.

5 A state-of-the-art solution for preventing misuse of such transponders or smart posters which must operate only at a specific, designated location is to protect the smart poster or at least the transponder against illegal theft by structural (hardware) means, for example, by providing theft protection in the form of proof glass, so that the smart poster/transponder is protected against theft and vandalism. This solution has the disadvantage that it is very costly for the operator of the transponder.

10 Especially when the smart poster applications are time-terminated applications, i.e. the data provided by the transponder are only valid for a certain period of time, it is required that the smart posters or the transponder are removed or that at least the transponder has to be deactivated when the smart poster application has been terminated. Structural (hardware) means for protecting the transponder/smart poster against theft has to consider this aspect, which also affects the operational costs.

15

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a method, a transponder, a transceiver, a poster, and a poster wall of the type mentioned in the opening paragraph, which obviate the drawbacks described above.

20 In particular, it is an object of the invention to provide a cheap and easy-to-install solution which allows preventing misuse of such transponders or smart posters which must operate only at a specific, designated location.

To achieve the object described above, a method according to the invention has such characteristic features that it can be characterized as follows:

25 A method of reading data from a first transponder into a transceiver, wherein the transceiver performs the following steps when said first transponder and a second transponder are within the RFID communication range of the transceiver at the same time:

- receiving exchange information from the first transponder after sending a request for transmitting data to said first transponder,
- 30 - transmitting said exchange information to said second transponder,
- receiving encrypted information from the second transponder, which encrypted information represents the exchange information of the first transponder, scrambled with a key of the second transponder,
- transmitting said encrypted information to the first transponder, and

- provided that the first transponder permits access to the data, receiving the requested data from the first transponder.

The inventive object is also solved by a transponder for communicating with a further transponder via a transceiver, wherein the transponder comprises

- 5 - means for generating exchange information,
- means for transmitting said exchange information to a transceiver,
- means for receiving encrypted information from said transceiver,
- means for decrypting said encrypted information, and
- 10 - means for comparing the resulting information of the decryption of the encrypted information with the exchange information generated with the generating means.

The object of the invention is further solved by a transponder for communicating with a further transponder via a transceiver, wherein the transponder comprises

- 15 - means for receiving exchange information from a transceiver,
- means for encrypting said exchange information, and
- means for transmitting encrypted information resulting from the encryption of said exchange information to the transceiver.

Yet another solution for the inventive object is a transponder for communicating with a further transponder via a transceiver, wherein the transponder comprises

- 20 - means for generating exchange information,
- means for transmitting said exchange information and for transmitting encrypted information resulting from the encryption of received exchange information to the transceiver,
- 25 - means for receiving encrypted information and for receiving exchange information from a transceiver,
- means for decrypting said encrypted information,
- means for comparing the resulting information of the decryption of the encrypted information with the exchange information generated with the generating means,
- 30 and
- means for encrypting said exchange information.

To achieve the inventive object, also a transceiver for controlling the communication of two transponders is disclosed, wherein the transceiver comprises

- means for receiving exchange/encrypted information from the first/second

transponder, and

- means for transmitting, to the second/first transponder, exchange/encrypted information received from the first/second transponder, which exchange/encrypted information is intended to be transmitted to the second/first transponder.

5 Yet another solution for the inventive object is a transceiver, which comprises means for receiving data from one of the transponders.

Finally, the object of the invention is solved by a poster, wherein a transponder is attached to said poster, as well as by a poster wall comprising said poster.

10 The provision of the characteristic features according to the invention creates the advantage that the transceiver is provided with data from a first transponder only if said transponder is close to a second transponder, i.e. both transponders have to be within the communication range of the transceiver. In this case, communication of the transponders via the transceiver will take place when the transceiver comes close to the transponders. The first transponder which carries the data verifies if the second transponder is present and access is
15 granted to the data stored on said first transponder only if the presence of the second transponder can be verified. Access to the data stored on the first transponder is automatically disabled when the first transponder is removed from the second one.

The invention offers the advantage that it is not necessary to secure the first transponder against theft by using other cost-intensive solutions such as structural means.
20 The invention therefore allows mobility of the first transponder.

The solution according to the invention uses standardized communication between a transponder and a transceiver as well as a standard authentication procedure which is well-known in the state of the art between a transponder and a transceiver so that the invention may be realized within an existing transceiver infrastructure. However, since such
25 an authentication works at any place where the transponder and the transceiver come close together, a second transponder is used, so that an authentication is only possible if both transponders are within the communication range of the transceiver at the same time.

It is also known in the state of the art that a further server which is capable of communicating with the transponder via the transceiver is used for an authentication
30 procedure, and US 6,717,507 discloses a method of accessing and controlling a media source by reading out information from a transponder with a reader.

However, all of these known solutions are not suitable to avoid removal of a transponder from a specific location because the functioning of the authentication of a transponder or access to, or control of, a media source does not depend on the position of the

transponder with respect to the server or on the position of the media source with respect to the position of the transponder.

However, concerning the invention as claimed, it is necessary that both transponders are within the RFID communication range at the same time so that the authentication procedure can work. When a transponder is removed from its position, the authentication will not work anymore and access to the data stored on the first transponder is denied.

It is advantageous when the transceiver performs the following steps after sending the request to the first transponder and before receiving said exchange information from the first transponder:

- receiving further, first exchange information from the second transponder,
- transmitting said first exchange information to the first transponder,
- receiving first encrypted information from the first transponder, which first encrypted information represents the exchange information of the second transponder, scrambled with a key of the first transponder, and
- transmitting said first encrypted information to the second transponder.

This provides an additional authentication procedure between the two transponders. Such an authentication procedure makes it possible that the first transponder and the second transponder are operated by different persons, organizations or enterprises, because the service offered by the second transponder, namely that the first transponder only provides data to a reader when the second transponder is close to the first transponder, may only be claimed if the first transponder authenticates itself to the second transponder.

It is also advantageous when the second transponder is a stationary, immobile transponder. This provides the advantage that it is not possible for a malicious person to remove the first and the second transponder together. Providing structural means against theft of the second transponder will involve additional costs. However, since in contrast to the first transponder, the second transponder usually has to be installed only once, these measures increase security at relatively low cost.

Yet another beneficial solution is a method wherein the exchange information is a random number. The security of communication can thereby be improved because the use of a random number as exchange information provides the advantage that so-called "replay attacks" are not possible.

Furthermore, it is advantageous when both transponders are passive transponders and/or when the first and the second transponder are identical. This provides the advantage of low cost.

It is also beneficial when the transponder comprises memory means for storing data and/or for storing keys being used in the encryption and/or decryption of exchange/encrypted information. The authentication process can thus take place very fast as keys do not have to be fetched from a remote location.

It is also advantageous when the transceiver comprises means for receiving data from one of the transponders.

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in greater detail hereinafter, by way of non-limiting example, with reference to the embodiments shown in the drawings.

Fig. 1 shows a possible application of the invention.

Fig. 2 shows a first and a second transponder communicating via a transceiver according to the invention.

Fig. 3 is a flow chart of a first embodiment of the method according to the invention.

Fig. 4 is a flow chart of a second embodiment of the method according to the invention.

DESCRIPTION OF EMBODIMENTS

Fig. 1 shows a poster POS with the schedule of a public transportation system. A first transponder TAG1 is attached to said poster POS. To buy a ticket for the public transportation system, a user brings his transceiver REA close to the first transponder TAG1 so that the relevant data dat (See Fig. 2) may be transferred from the first transponder TAG1 to the transceiver REA.

It should be noted that the relevant data dat may be stored directly on the first transponder TAG1. However, it is also possible that only a reference, such as a URL to said data dat is stored on the first transponder TAG1 and that the data itself are stored on a remote server. The reader REA may then obtain said data from the server using said reference such as a URL, for example, by establishing a GPRS connection to said reference. In the context

of this document, both situations will be covered by the phrase “data dat being stored on the first transponder TAG1”.

The poster POS is attached to a poster wall WAL. A second transponder TAG2 is attached to said poster wall WAL so that the first transponder TAG1 and the second transponder TAG2 are close together. Both transponders TAG1, TAG2 are RFID-tags which are preferably passive. Furthermore, it is possible that identical transponders TAG1, TAG2 are used.

A user who wants to read data dat from the first transponder TAG1 has to “touch” the first transponder TAG1 with his transceiver REA, which means that he has to bring his transceiver REA close to the first transponder TAG1 so that the first transponder TAG1 is within the RFID communication range of the transceiver REA.

Since the first transponder TAG1 and the second transponder TAG2 are close together, both transponders TAG1, TAG2 are powered and operated within one electromagnetic field generated by the transceiver REA. The transceiver REA is capable of communicating to each transponder TAG1, TAG2 individually and communication of the two transponders TAG1, TAG2 can be realized via the reader REA. The transceiver REA thus controls the communication of the two transponders TAG1, TAG2.

The second transponder TAG2 is non-detachably arranged on the poster wall WAL which is protected against theft and vandalism of the second transponder TAG2, e.g. the second transponder TAG2 is positioned in a concrete block of the poster wall WAL or the second transponder TAG2 is protected against theft and/or vandalism by other structural means such as proof glass.

The essential idea of the invention is that the first transponder TAG1 declines communication access to the transceiver REA as long as the second transponder TAG2 has not authenticated the first transponder TAG1. Thus the first transponder TAG1 only grants access to the data stored on it if the second transponder TAG2 authenticates the first transponder TAG1 by applying proper cryptographic protocols. This arrangement binds the first transponder TAG1 to the designated location by logical means rather than by structural means.

The poster POS and the corresponding first transponder TAG1 and the poster wall WAL with the second transponder TAG2 may be operated by the same operator. However, the poster POS and the poster wall WAL will usually be operated by different operators. The first transponder TAG1 may be operated by a first enterprise (“application provider”) which offers a certain application by storing corresponding data dat on the first

transponder TAG1, which data dat can be read from the first transponder. In the present case, the application provider allows buying a mobile ticket for the public transportation system. The second transponder TAG2 is operated by a second enterprise ("service provider").

Before communication according to the invention may be established, it is
5 necessary to "personalize" the different transponders. This means that the key or keys of the "application provider" and the "service provider" necessary for a positive authentication procedure have to be stored on the corresponding transponders.

The personalization of the first transponder TAG1 should be carried out in a safe and secure environment, for example, in the poster printing plant, in the poster delivery
10 station or during placement of the poster POS at the poster wall WAL ("Pre-Issuance personalization in a secure environment").

Fig. 2 shows, in greater detail, a first transponder TAG1 and a second transponder TAG2 communicating via a transceiver REA. The first transponder TAG1 comprises sending/receiving means SER1 for sending information such as exchange
15 information C2 and encrypted information R1 to the transceiver REA. Furthermore, said sending/receiving means SER1 are adapted to receive information such as exchange information C1 and encrypted information R2 from the transceiver REA.

The first transponder TAG1 also comprises means RAN1 for generating exchange information C2, which exchange information C2 is usually a random number.
20 Furthermore, encoding/decoding means ENC/DEC1 are provided for encrypting exchange information C1 received from the second transponder TAG2 via the transceiver REA into encrypted information R1 and for decrypting encrypted information R2 received from the second transponder TAG2 via the transceiver REA into decrypted information C2'.

The first transponder TAG1 further comprises means COMP1 for comparing
25 the exchange information C2, generated with the exchange information-generating means RAN1, and the above-mentioned decrypted information C2'. Finally, memory means MEM1 are provided for storing data dat and keys K1s, K2p which are necessary for the authentication procedures according to the invention.

The second transponder TAG2 comprises sending/receiving means SER2 for
30 sending information such as exchange information C1 and encrypted information R2 to the transceiver REA. Furthermore, said sending/receiving means SER2 are adapted to receive information such as exchange information C2 and encrypted information R1 from the transceiver REA.

The second transponder TAG2 also comprises means RAN2 for generating exchange information C1 which is usually a random number. Furthermore, encoding/decoding means ENC/DEC2 are provided for encrypting exchange information C2 received from the first transponder TAG1 via the transceiver REA into encrypted information R2 and for decrypting encrypted information R1 received from the first transponder TAG1 via the transceiver REA into decrypted information C1'.

The second transponder TAG2 further comprises means COMP2 for comparing the exchange information C1, generated with the exchange information-generating means RAN2, and the above-mentioned decrypted information C1'. Finally, memory means MEM2 are provided for storing keys K1p, K2s which are necessary for the authentication procedures according to the invention.

Asymmetric ciphering as well as symmetric ciphering may be used in the communication process between the two transponders TAG1, TAG2. In the case of symmetric ciphering, the keys for encrypting and decrypting are identical, which makes it necessary that the keys are exchanged in a secure environment. Symmetric ciphering provides the advantage that only little "computing power" is necessary and that there are only small memory requirements as far as the memory of the transponders is concerned. However, asymmetric ciphering provides the advantage that it is not necessary that keys are exchanged in a secure environment.

In Fig. 2, it is assumed that asymmetric ciphering is used, with a first pair of a public key K1p and a secret key K1s of the first transponder TAG1 and a second pair of a public key K2p and a secret key K2s of the second transponder TAG2. The secret key K1s of the first transponder TAG1 and the public key K2p of the second transponder TAG2 are stored on the first transponder TAG1, whereas the secret key K2s of the second transponder TAG2 and the public key K1p of the first transponder TAG1 are stored on the second transponder TAG2.

Fig. 2 also depicts a transceiver REA which comprises sending/receiving means SER designed to receive and send information C1, C2, R1, R2 as well as data dat from the first and the second transponder TAG1, TAG2.

Fig. 3 shows the main aspects of a method according to the invention in a simple manner. First of all, the transceiver REA sends a request req to the first transponder TAG1, with which request req the transceiver REA requests the transmission of data dat stored on the first transponder TAG1. The first transponder TAG1 denies this request and generates exchange information C2 which is then transmitted to the transceiver REA. The

transceiver REA transmits the exchange information C2 to the second transponder TAG2, where said exchange information C2 is encrypted to encrypted information R2. Said encrypted information R2 is now transmitted to the first transponder TAG1 via the transceiver REA.

5 The first transponder TAG1 decrypts said encrypted information R2 to decrypted information C2'. Said decrypted information C2' is compared with the original exchange information C2. When the original information C2 and the decrypted information C2' are identical, the first transponder TAG1 transmits the data dat requested to the transceiver REA.

10 Since this authentication procedure only works when the first transponder TAG1 and the second transponder TAG2 are close together within the RFID communication range of the transceiver REA, the first transponder TAG1 will provide the data dat stored on it to a transceiver REA only in a certain, well-defined region.

 A method as described in Fig. 3 is used when both transponders TAG1, TAG2
15 are operated by the same "provider". Especially when symmetric ciphering is used and the used key for encryption and decryption is secret, the service of "binding the first transponder TAG1 to a specific location" can only be provided to the owner of the secret key.

 When the transponders TAG1, TAG2 are operated by different providers, an additional authentication procedure is advantageous, which will be explained in detail in
20 Fig. 4. In Fig. 4, it is assumed that asymmetric ciphering is applied. According to the method as shown in Fig. 4, the transceiver REA sends a request req to the first transponder TAG1. The first transponder TAG1 requests exchange information from the second transponder TAG2 by transmitting a get-signal get to the second transponder TAG2 via the transceiver REA. The second transponder TAG2 transmits exchange information C1 to the first
25 transponder TAG1 via the transceiver REA.

 The first transponder TAG1 encrypts said exchange information C1 to encrypted information R1 with the secret key K1s. Said encrypted information R1 is transmitted to the second transponder TAG2 via the transceiver REA. Furthermore, exchange information C2 of the first transponder TAG1 is transmitted to the second transponder TAG2.

30 The second transponder TAG2 first decrypts the encrypted information R1 from the first transponder TAG1 to decrypted information C1' with the public key K1p, which decrypted information C1' is then compared with the original exchange information C1 sent to the first transponder TAG1. When both information C1, C1' is identical, the authentication of first transponder TAG1 to the second transponder TAG2 has been

successful. In the case of a successful authentication, the second transponder TAG2 then encrypts the exchange information C2 received from the first transponder TAG1 with the secret key K2s to encrypted information R2 which is then transmitted to the first transponder TAG1 via the transceiver REA.

5 The first transponder TAG1 decrypts said encrypted information R2 to decrypted information C2' with the public key K2p. Said decrypted information C2' is compared with the original exchange information C2. When the original information C2 and the decrypted information C2' are identical, the first transponder TAG1 transmits the data dat requested to the transceiver REA.

10 Since this authentication procedure only works when the first transponder TAG1 and the second transponder TAG2 are close together within the communication range of the transceiver REA, the first transponder TAG1 will provide the data dat stored on it to a transceiver REA only in a certain, well-defined region.

15 The advantages obtained by the inventive solution as compared to state-of-the-art solutions are as follows.

- Low cost, all transponders may be passive tags.
- It is not mandatory that the second transponder TAG2 stores application-specific data; hence, application-specific personalization of the second transponder TAG2 is superfluous. The operational costs for the second transponder TAG2 will be reduced to a
20 minimum.
- The application-specific personalization of the first transponder TAG1 can be performed within production time. It is not mandatory to personalize the first transponder TAG1 in the field (post-issuance personalization). This has the advantage that erroneous personalization in the field is not possible.
- 25 - Simplicity: The key management is simple. The easy key management enables separate providers for the first transponder TAG1 and the second transponder TAG2. The operator of the first transponder TAG1 and the operator of the second transponder TAG2 do not need to work under the same trust model, i.e. they do not need to share a common secret key. A security-relevant key exchange and thus a complicated process of key exchange
30 are superfluous.
- Simplicity: Placement of the (smart) poster POS does not need any mechanical protection.

- Security: The posters POS are safeguarded against removal from the designated poster location. The invention provides protection against placement of posters at unwanted locations.

5 It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be construed as limiting the claims. Use of the verb "comprise" and its conjugations does not
10 exclude the presence of elements or steps other than those stated in any claim or the specification as a whole. The singular reference of an element does not exclude the plural reference of such elements, and vice-versa. In a device claim enumerating several means, several of these means may be embodied by one and the same item of hardware or software. The mere fact that certain measures are recited in mutually different dependent claims does
15 not indicate that a combination of these measures cannot be used to advantage.

15

CLAIMS:

1. A method of reading data (dat) from a first transponder (TAG1) into a transceiver (REA), wherein the transceiver (REA) performs the following steps when said first transponder (TAG1) and a second transponder (TAG2) are within the RFID communication range of the transceiver (REA) at the same time:
- 5 - receiving exchange information (C2) from the first transponder (TAG1) after sending a request (req) for transmitting data (dat) to said first transponders (TAG1),
- transmitting said exchange information (C2) to said second transponder (TAG2),
- 10 - receiving encrypted information (R2) from the second transponder (TAG2), which encrypted information (R2) represents the exchange information (C2) of the first transponder (TAG1), scrambled with a key (K2) of the second transponder (TAG2),
- transmitting said encrypted information (R2) to the first transponder (TAG1), and
- 15 - provided that the first transponder (TAG1) permits access to the data (dat), receiving the requested data (dat) from the first transponder (TAG1).
2. A method as claimed in claim 1, wherein the transceiver (REA) performs the following steps after sending the request (req) to the first transponder (TAG1) and before
- 20 receiving said exchange information (C2) from the first transponder (TAG1):
- receiving further, first exchange information (C1) from the second transponder (TAG2),
- transmitting said first exchange information (C1) to the first transponder (TAG1),
- 25 - receiving first encrypted information (R1) from the first transponder (TAG1), which first encrypted information (R1) represents the exchange information (C1) of the second transponder (TAG2), scrambled with a key (K1) of the first transponder (TAG1), and
- transmitting said first encrypted information (R1) to the second transponder (TAG2).
- 30

3. A method as claimed in claim 1 or 2, wherein the second transponder (TAG2) is a stationary, immobile transponder.
4. A method as claimed in claim 1 or 2, wherein the exchange information (C1,
5 C2) is a random number.
5. A method as claimed in claim 1 or 2, wherein the first and the second transponder (TAG1, TAG2) are passive transponders.
- 10 6. A method as claimed in claim 1 or 2, wherein the first and the second transponder (TAG1, TAG2) are identical.
7. A transponder (TAG1, TAG2) for communicating with a further transponder (TAG2, TAG1) via a transceiver (REA), wherein the transponder (TAG1,
15 TAG2) comprises
- means (RAN1, RAN2) for generating exchange information (C2, C1),
 - means (SER1, SER2) for transmitting said exchange information (C2, C1) to a transceiver (REA),
 - means (SER1, SER2) for receiving encrypted information (R2, R1) from said
20 transceiver (REA),
 - means (ENC/DEC1, ENC/DEC2) for decrypting said encrypted information (R2, R1), and
 - means (COMP1, COMP2) for comparing the resulting information (C2', C1') of the decryption of the encrypted information (R2, R1) with the exchange information (C2,
25 C1) generated with the generating means (RAN1, RAN2).
8. A transponder (TAG1, TAG2) for communicating with a further transponder (TAG2, TAG1) via a transceiver (REA), wherein the transponder (TAG1, TAG2) comprises
- 30 - means (SER1, SER2) for receiving exchange information (C1, C2) from a transceiver (REA),
- means (ENC/DEC1, ENC/DEC2) for encrypting said exchange information (C1, C2), and
 - means (SER1, SER2) for transmitting encrypted information (R1, R2)

resulting from the encryption of said exchange information (C1, C2) to the transceiver (REA).

9. A transponder (TAG1, TAG2) for communicating with a further transponder (TAG2, TAG1) via a transceiver (REA), wherein the transponder (TAG1, TAG2) comprises
- means (RAN1, RAN2) for generating exchange information (C2, C1),
 - means (SER1, SER2) for transmitting said exchange information (C2, C1) and for transmitting encrypted information (R1, R2) resulting from the encryption of received exchange information (C1, C2) to the transceiver (REA),
 - means (SER1, SER2) for receiving encrypted information (R2, R1) and for receiving exchange information (C1, C2) from a transceiver (REA),
 - means (ENC/DEC1, ENC/DEC2) for decrypting said encrypted information (R2, R1),
 - means (COMP1, COMP2) for comparing the resulting information (C2', C1') of the decryption of the encrypted information (R2, R1) with the exchange information (C2, C1) generated with the generating means (RAN1, RAN2), and
 - means (ENC/DEC1, ENC/DEC2) for encrypting said exchange information (C1, C2).

10. A transceiver (REA) for controlling the communication of two transponders (TAG1, TAG2), wherein the transceiver (REA) comprises
- means (SER) for receiving exchange/encrypted information (R1, R2, C1, C2) from the first/second transponder (TAG1, TAG2), and
 - means (SER) for transmitting, to the second/first transponder (TAG2, TAG1), exchange/encrypted information (R1, R2, C1, C2) received from the first/second transponder (TAG1, TAG2), which exchange/encrypted information (R1, R2, C1, C2) is intended to be transmitted to the second/first transponder (TAG2, TAG1).

11. A poster (POS), wherein a transponder (TAG1) as claimed in one of the claims 7 to 9 is attached to said poster (POS).

12. A poster wall (WAL), wherein a poster (POS) as claimed in claim 11 and a transponder (TAG2) as claimed in claim 8 or 9 are attached to said poster wall (WAL).

1/4

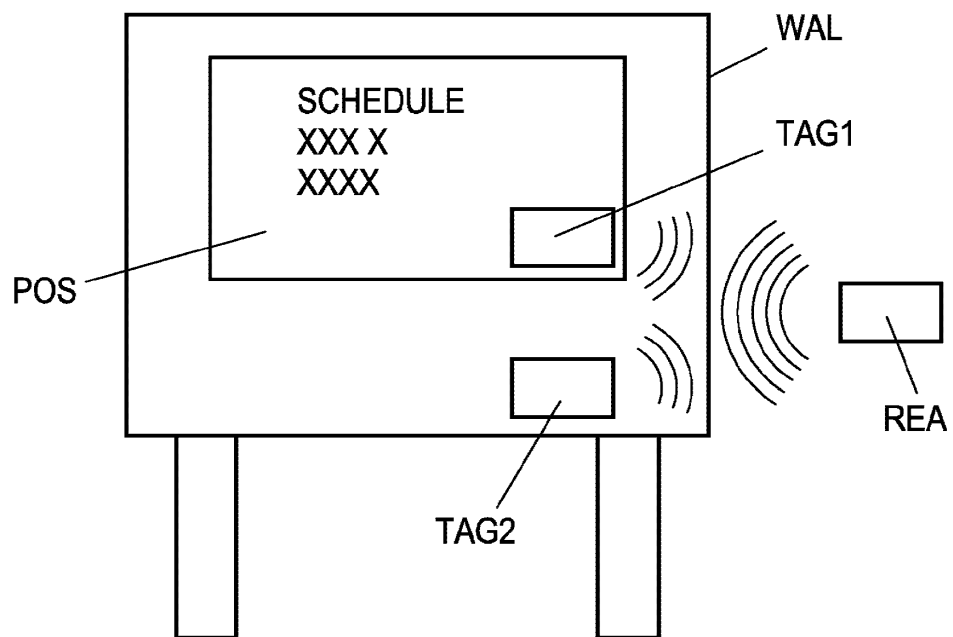


FIG. 1

2/4

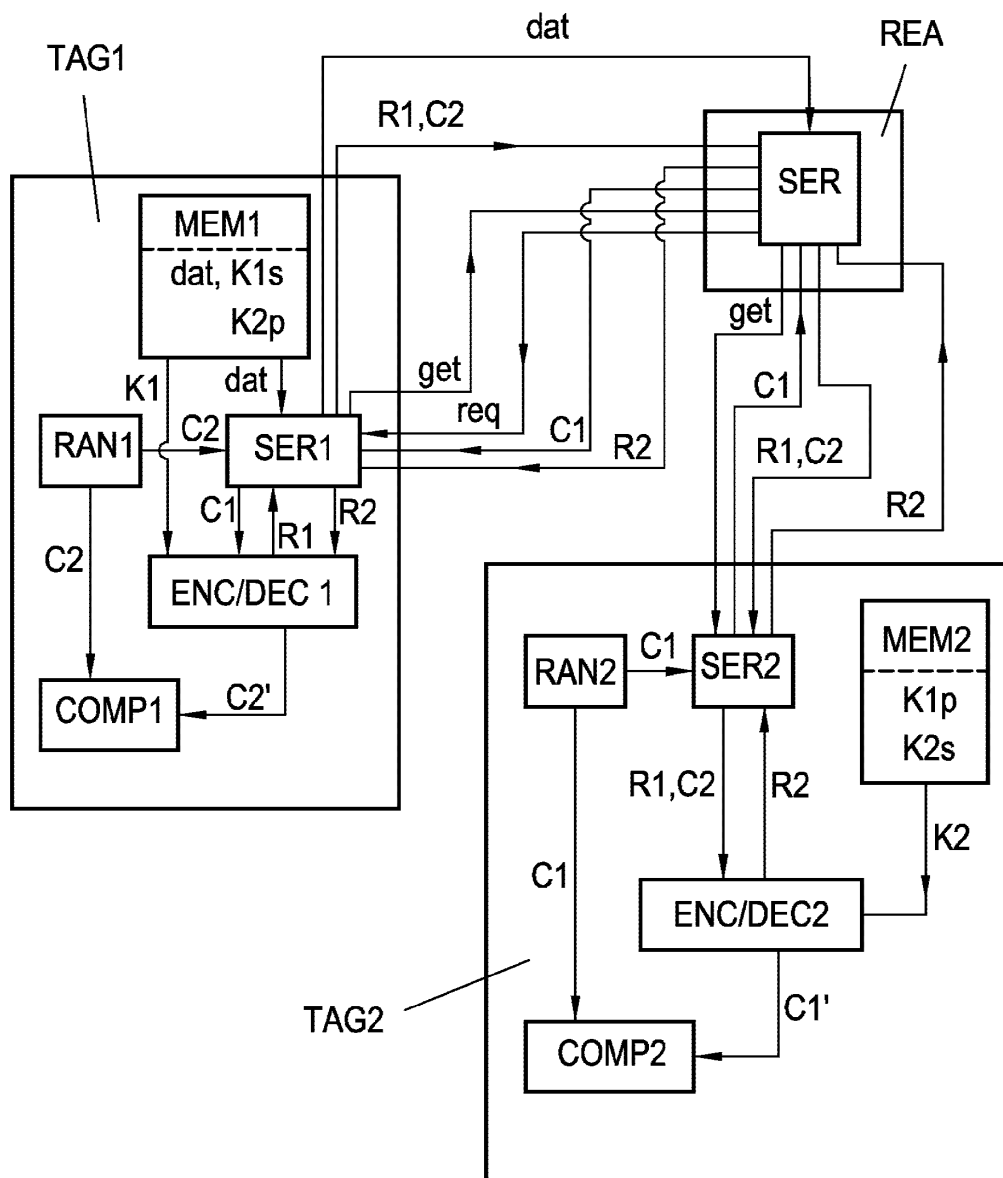


FIG. 2

3/4

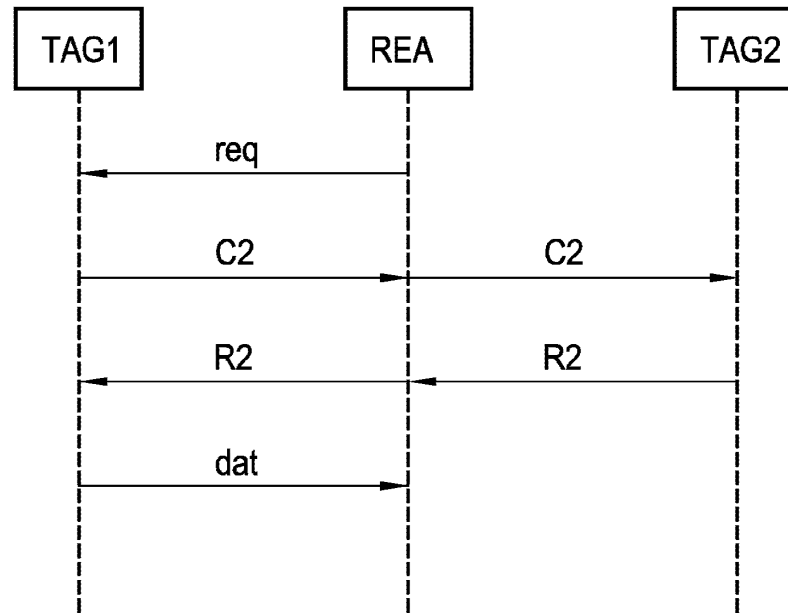


FIG. 3

4/4

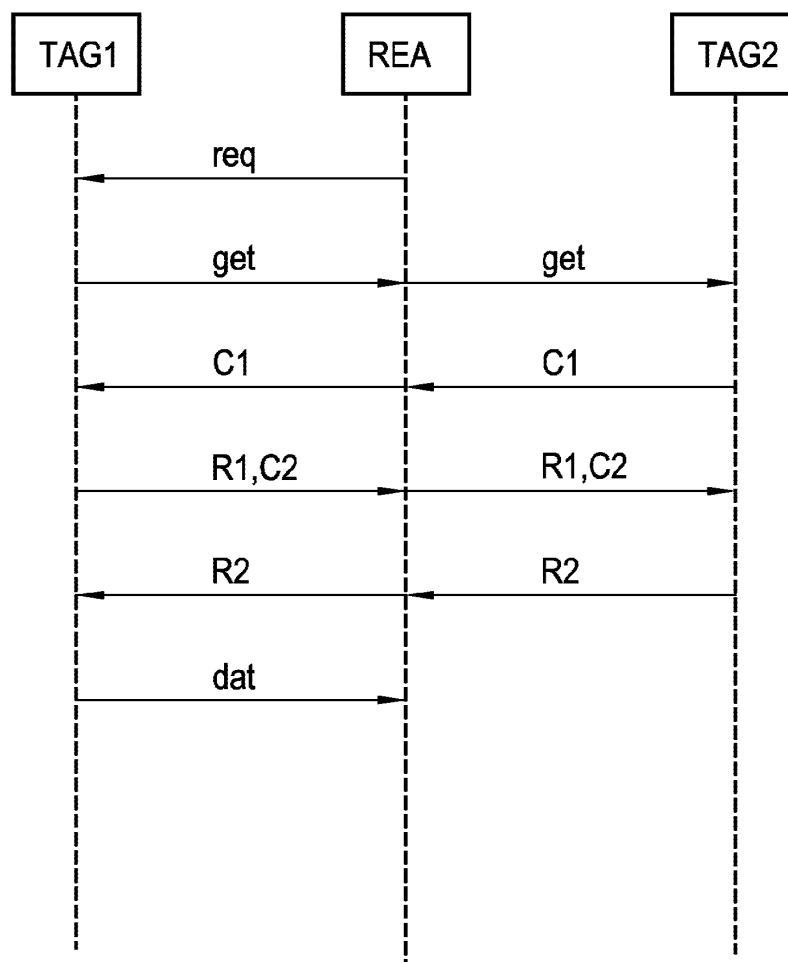


FIG. 4

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 August 2007 (23.08.2007)

PCT

(10) International Publication Number
WO 2007/094868 A2

(51) International Patent Classification: **Not classified**

(21) International Application Number:
PCT/US2006/060339

(22) International Filing Date: 27 October 2006 (27.10.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/731,629 28 October 2005 (28.10.2005) US

(71) Applicant (for all designated States except US): **MOJIX, INC.** [US/US]; 11075 Santa Monica Boulevard, Suite 350, Los Angeles, CA 90025 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SADR, Ramin** [US/US]; 1034 Somera Road, Los Angeles, CA 90077 (US).

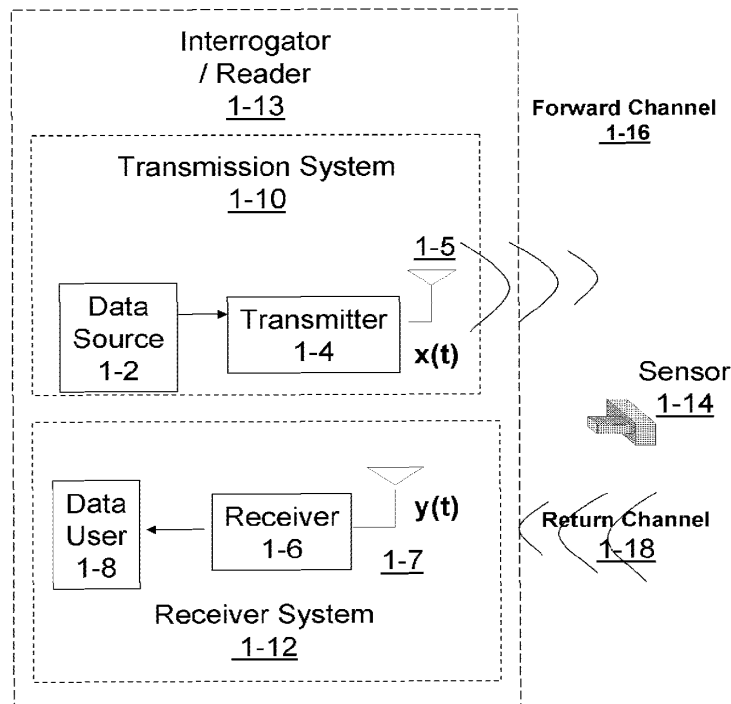
(74) Agents: **BRUNELL, Norman E.** et al.; Irell & Manella LLP, 1800 Avenue of the Stars, Suite 900, Los Angeles, CA 90067 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: RFID RECEIVER



(57) Abstract: RFID data signals from RFID tags may be recovered by determining the probabilities of transitions between data states between a series of a pairs of signal samples using a set of predetermined probabilities related to data, timing, baud rate and/or phase variables affecting the received signal and processing those determined probabilities to determine the sequence of such transitions that has the highest probability of occurrence. A second set of predetermined probabilities related to transitions in the opposite direction may be used to sequence in a reverse direction. The determination of the sequence representing the RFID tag data may be iterated in both directions until further iterations don't change the determined probabilities.

WO 2007/094868 A2



RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

RFID RECEIVER

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U. S. provisional application Serial No. 60/731,629 filed October 28, 2005.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] This invention is related to transmitter – receiver systems and in particular is related to systems for the detection of signals in difficult environments such as for use in sensory networks and Radio Frequency Identification (RFID) systems.

2. Description of the Prior Art

[0003] The detection of signals in difficult environments, such as where the signal to noise ratio is very low and/or the interference from other signals is very high, has always been a substantial problem. In many systems today classical detection theory is used in digital transceivers. In these systems the bit stream embedded in information bearing signal is detected one-bit at a time using a "matched filter" designed to match the signal waveform at the input of the receiver.

[0004] What is needed is a robust and powerful method for the detection of extremely weak signals with severe phase and timing ambiguities due to the source characteristics and propagation environment. The proposed system has a substantial superior performance than the classical signal detector.

SUMMARY OF THE INVENTION

[0005] In a first aspect, a method for operating an RFID receiver may include sampling a received signal including RFID data signals from at least one interrogated RFID tag, providing a set of predetermined probabilities of a received signal sample making a specific transition between data states, each predetermined probability related to data, timing and baud rate variables affecting the received signal, applying the set of predetermined probabilities to each of a plurality of pairs of signal samples to determine probabilities of the received signal having made the specific transitions between each of the signal samples in that pair and processing the determined probabilities to recover RFID data signals by determining a sequence of transitions in the received signal having the highest probability of occurrence.

[0006] The predetermined probabilities may also be related to a phase variable affecting the received signal. The applying the set of predetermined probabilities, and the processing the determined probabilities, may be iterated to recover the RFID data signals. The set of predetermined probabilities may be related to transitions in a first direction. A second set of predetermined probabilities related to transitions in an opposite direction may be provided and applied to each of the plurality of pairs of signal samples to determine second probabilities of the received signal making the specific transitions between each of the signal samples in that pair in the opposite direction and the first and second determined probabilities may be processed to recover the RFID signals. Applying the first and second set of predetermined probabilities, and the processing the first and second determined probabilities, may be iterated to recover the RFID data signals. The applying and processing may be iterated until further iterations do not further change the determined probabilities.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0007] Fig. 1 is a simplified block diagram of an RF transmitter-receiver system and passive sensor.
- [0008] Fig. 2a is a simplified block diagram of an end to end communication system of the type shown in Fig. 1.
- [0009] Fig. 2b is a model of a SISO implementation of the system shown in Fig. 2a.
- [0010] Fig. 3 is a diagram of a SISO decoder as a 4-Port Device.
- [0011] Fig. 4 is a block diagram of SISO processing with interleaving and de-interleaving.
- [0012] Fig. 5 is an illustration of Quantized Phase Space.
- [0013] Fig. 6 is an illustration of Quantized Time Domain.
- [0014] Fig. 7 is an illustration of Example of Trellis Diagram.
- [0015] Fig. 8a is an illustration of a Single State Trellis Transition
- [0016] Fig. 8b is an illustration of a Trellis Section.
- [0017] Fig. 9a is a block diagram of Single Parity Check Code (SPC).
- [0018] Fig. 9b is a block diagram of an RFID SISO Decoder.
- [0019] Fig. 9c represents the detailed operation of a SISO decoder for repetition code.
- [0020] Fig. 9d illustrates the operation of a SISO decoder for SPC.
- [0021] Fig. 10 is a block Coherent SISO Decoder.
- [0022] Fig. 11 is a block Non-Coherent SISO Decoder.
- [0023] Fig. 12a illustrates a block Cascaded Non-Coherent.
- [0024] Fig. 12b illustrates a Coherent SISO Decoder.
- [0025] Fig. 13a is a block diagram of an RFID System.
- [0026] Fig. 13b is a block diagram of a reader/interrogator of Fig. 13a.
- [0027] Fig. 14a is block diagram of FM0 encoder for RFID applications.
- [0028] Fig. 14b is block diagram of Miller encoder for RFID applications.
- [0029] Fig. 15a is a block diagram of classical coherent detector.
- [0030] Fig. 15b is a block diagram of classical non-coherent detector.
- [0031] Fig. 15c is a block diagram of a multiple symbol non-coherent detector.
- [0032] Fig. 15d illustrates the operation of the multiple symbol non-coherent detector of Fig. 15c.

- [0033]** Fig. 16 shows a trellis diagram for FM0 and Miller code.
- [0034]** Fig. 17 shows a bit error rate as function of signal-to-noise ratio.
- [0035]** Fig. 18 shows a first method for a timing trellis section for pulses with time varying duration.
- [0036]** Fig. 19 shows timing tick marks for the method Fig. 18.
- [0037]** Fig. 20 shows a second method using a folded timing trellis for pulses with time varying duration.
- [0038]** Fig. 21 shows a tree diagram with three transitions per node.
- [0039]** Fig. 22 shows an example of a symbol tree structure method 3 for $N=4$, and $\Delta_{\max}=1$.
- [0040]** Fig. 23 shows an example of symbol tree with windowed structure method 3 for $N=4$, and $\Delta_{\max}=1$.
- [0041]** Fig. 24 shows a SISO implementation: Intermediate metric variable computation.
- [0042]** Fig. 25 shows a SISO implementation: Interconnect of node processors and branch select units.
- [0043]** Fig. 26 shows a SISO implementation: Extended parallel source node processing.
- [0044]** Fig. 27 shows a Forward and Backward processor.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

[0045] Receiver subsystems may provide enhanced detection of signals where some latency may be tolerated, particularly for use in sensory networks and passive Radio Frequency Identification (RFID) based systems. Such systems may use iterative processing techniques with soft-input-soft-output (SISO) components to combine channel decoding with equalization, demodulation, phase tracking, symbol timing and synchronization and interference cancellation. This is achieved with exchange of probabilities or "soft information" or equivalently the probability of correct detection of transmitted symbols based on the observed vector, at any given state of a finite state machine (FSM) which models the observation space. The evolution of FSM in time domain results into a planar graph referred to here as the "Trellis". In the presence of additive white Gaussian noise (AWGN) with random phase and timing, the performance of the receiver using SISO approaches that of an ideal coherent receiver. In the presence of other channel anomalies such as multipath, fading and jamming, the performance gain is much greater than conventional systems. The SISO decoders described here can also be used for applications where serial or parallel concatenated channel coding methods is employed.

[0046] The system disclosed herein may use iterative algorithms that can be applied to a broad range of sensory class of signals and waveforms. Iterative processing techniques with soft-input-soft-output (SISO) components may be used to combine channel decoding with equalization, demodulation, phase tracking, symbol timing and synchronization and interference cancellation. This is achieved with exchange of probabilities or "soft information". When the transmitted sequence is produced from a binary symmetric source (BSS) and in presence of additive white Gaussian noise (AWGN), channel distortion, random phase and synchronization error, the performance of the receiver converges to the ideal coherent receiver for un-coded signal. In presence of other channel anomalies such as multipath, fading and jamming, the expected performance gain is much greater than conventional systems. The overall SISO decoders described here can also be used for applications where serial or parallel concatenated channel coding methods are employed.

[0047] Referring now to Fig. 1, transmission system 1-10 transmits a signal in forward channel 1-16, such as an RF channel, which is applied to sensor 1-14 which may be an RFID tag. The transmitted signal $x(t)$ in forward channel 1-16 may be modeled as the real part of

the complex transmitted signal, that is $x(t) = \text{Real}[a(t)e^{j(\omega_c t + \theta)}]$ for $t \in [nT_{\text{sym}}, (n+1)T_{\text{sym}})$; where T_{sym} denotes the symbol time interval, $a(t)$ may be complex or real-valued information bearing signal and θ denotes the phase of the transmitted signal during the symbol time. This phase can be time varying from symbol to symbol. In passive RFID tag applications, the transmitted and received waveforms are independent, however, the power transmitted from the tag 1-14 depends on the power of the signal from the reader and the tag efficiency to convert its received power to available transmit power back to the reader. In active sensors, the transmitted and received signals are typically mutually independent signals.

[0048] Transmission system 1-10 includes data source 1-2 of transmission system 1-10 is used to modulate transmitter 1-4. Antenna 1-5 applies the modulated signal through forward channel 1-16 to the sensor 1-14. Typically in RFID applications the transmitter 1-4 and the data source 1-2 form the interrogator or the reader in RFID networks. Data source 1-2 is used by the reader to embed an address and/or command sequence to the device such as RFID tag 1-14. In backscatter passive RFID tags, the transmitted signal may also embed a sinusoidal signal with a continuous waveform (CW), which may be used to supply power to passive RFID tag. RFID tag 1-14 may then respond back with a data sequence, based on the received command, through the air which is illustrated as the Return Channel 1-18. The main function of the receiver system 1-12 is to detect the data transmitted from the sensor 1-14, in presence of various distortions encountered in the return channel 1-18 such as multi-path and/or natural and man-made interference. Receiver system includes receiving antenna 1-7 which applies the signal received from RFID tag 1-14 to receiver 1-6. The detected data from receiver 1-6 may then be consumed by the user 1-8. In RFID applications the data user is the reader which passes the data to a higher layer protocol for interpretation of the received packet. For passive RFID tags, transmission system 1-10 and receiver system 1-12 may be referred to as "reader / interrogator" 1-13.

[0049] The underlying transmitter receiver pair, reader/interrogator 1-13, is shown in Fig. 1. The signal is transmitted over a communication channel with the impulse response $h(t)$ and corrupted with additive white Gaussian noise (AWGN) $n(t)$, the received signal $y(t)$ is modeled as:

$$y(t) = x(t) * h(t) + n(t) \quad (1)$$

where '*' represents the convolution operation.

[0050] Referring now to Fig. 2, an end-to-end communication system physical block diagram model 2-1 for a sensory signal is shown in Fig. 2a and includes data source 2-2 which feeds the modulator in the transmitter 2-4. This signal is applied via forward channel 2-6 to sensor 2-8. Only in the case when the transmitted signal from sensor 2-8 is a partially amplified version of the original signal, the impulse responses is the composite impulse response of the forward and return channel, i.e. $h_f(t) * h_r(t)$. In passive RFID applications, typically the tag may only use the signal from the reader to power itself. The return signal from the tag uses the backscatter modulation to modulate the electronic product code or a response back to the reader, in which case the channel impulse response is only limited to the return channel transfer function 2-10. The receiver 2-11 detects the incoming bit stream and outputs it to the user data 2-12.

[0051] In discrete time domain, we represent the sampled version of this complex received signal at time n as for the k^{th} packet or frame as an N -dimensional vector,

$$\mathbf{y}_k = H_k \mathbf{x}_k + \mathbf{n}_k \quad (2)$$

[0052] Here $\mathbf{y}_k$ denotes the received complex vector with dimension N obtained from uniform sampling of the received signal complex signal (after down-conversion) as $y(nT_s)$, where T_s denotes sampling interval, and the aggregate channel transfer function represented as

$$H = \begin{pmatrix} h_1 & 0 & \cdots & 0 \\ 0 & h_1 & h_2 & \cdots \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & h_1 \end{pmatrix} \quad (3)$$

[0053] Channel response matrix H may be real-or-complex valued constant, or belong to certain class of randomly distributed functions to model in-door or out-door multi-path channel response.

[0054] The sequence error probability may be minimized, which is equivalent to maximizing the a posteriori error probability conditioned on the sequence of observation. The estimated transmitted symbols are:

$$\hat{a}_n = \arg \max_{a_n \in \Psi} P(a_n | \mathbf{y}) \quad (4)$$

where, Ψ represents the input symbol alphabet.

By applying Bayes rule we have

$$P(a_k = \alpha | \mathbf{y}) = \sum_{\forall a \ni a_k = \alpha} \frac{P(\mathbf{y} | \mathbf{a})}{P(\mathbf{y})} P(\mathbf{a}). \quad (5)$$

If $\Psi = \{0, 1\}$ then let log likelihood ratio

$$\Lambda_1(a_n) = \log \frac{\Pr(a_n = 1 | \mathbf{y}_k)}{\Pr(a_n = 0 | \mathbf{y}_k)}. \quad (6)$$

Using Bayes formula and eliminating $\Pr(\mathbf{y})$, we obtain reliability or "extrinsic" information

$$\Lambda_1(a_n) = \lambda_1(a_n) + \lambda_2(a_n), \quad (7)$$

where $\lambda_1(a_n) = \log \frac{\Pr(\mathbf{y} | a_n = 1)}{\Pr(\mathbf{y} | a_n = 0)}$ represents the "extrinsic information" and

$\lambda_2(a_n) = \log \frac{\Pr(a_n = 1)}{\Pr(a_n = 0)}$ represents a priori log likelihood ratio (LLR) values. The sequence

$\lambda_1(a_n)$ is calculated in each iteration, and is the function of soft metric calculation block 4-8 shown in Fig. 4. In a SISO decoder, such as decoder 4-2 shown in Fig. 4, the a posteriori probability of each transmitted symbol may be computed and then subtracted from the reliability information to remove the influence of a priori information. The extrinsic information may then be fed back (and de-interleaved if channel encoding is used) for metric calculations for the next iteration, where:

$$\lambda_2(a_n) = \Lambda_2(a_n) - \tilde{\lambda}_1(a_n) = \log \frac{\Pr(a_n = 1 | \mathbf{y})}{\Pr(a_n = 0 | \mathbf{y})} \quad (8)$$

where tilde ($\sim$) denote values from the last decoding state. In presence of unknown random phase and timing, it may be necessary to consider the input and output joint probability

distribution functions $\Pr(\mathbf{a}, \boldsymbol{\phi}, \boldsymbol{\tau} | \mathbf{y})$ in which the optimization problem formulated in equation (4) becomes

$$(\hat{a}_n, \hat{\phi}_n, \hat{\tau}_n) = \arg \max_{(a_n, \phi_n, \tau_n) \in \Psi} P(a_n, \phi_n, \tau_n | \mathbf{y}) \quad (8a)$$

where, Ψ represents set of all values that a_n, ϕ_n, τ_n can take.

[0055] Referring now to Fig. 2b, in theoretical model 2-30, the performance of the overall RFID system may be enhanced by applying a simple and novel channel coding to the user data. This coding technique may include the use of an outer code 2-19, the interleaver 2-18 and a single parity check code 2-16, defined latter which is used to drive the modulation encoder over the channel. As an example, the outer code may be a repetition code (simply taking the input data of size M and repeating it q times where $q > 1$). The input data of size M bits may be partitioned into N equal size subsequences each of size M/N. Each subsequence is copied (repeated) q times (for example say $q=3$) then permuted by non-identical interleavers each of size M/N, all repeated and permuted subsequences enter a single parity check (SPC) with Nq input and one output. The output sequence of SPC may be of size M/N. the call output sequence may be considered as a parity sequence. Note that for this example the interleaver 2-18 is plurality of interleavers that can be more than one. The N data subsequences and the parity sequence may then be multiplexed to generate a sequence of length $M+M/N$ that enters the modulator encoder namely FM0, Miller, or any other modulator encoder used or to be used in the RFID system. It must be noted that 2-19, 2-18 and 2-16 are optional in the event it is desired to attain a coding gain in RFID systems.

[0056] The SISO decoder shown may be considered to be a device that maps an input sequence $\mathbf{a}$ to an output sequence $\mathbf{c}$ based on a finite state machine. If the coding scheme of 2-19, 2-18 and 2-16 is employed the SISO decoder will be designed to account for the outer code 2-19, interleaver 2-18, single parity code 2-16 and modulation encoder 2-14 when modeling the FSM for data encoder. The SISO decoder is embedded in the receiver 2-28. The outer code 2-19, the interleaver 2-18 and the single parity code 2-16 constitute a channel coding scheme that further take advantage of SISO decoder for the receiver realization in 2-28. A possible method of the channel coding technique for RFID applications is to apply the channel coding method to the RFID tag's identifier prior to writing into its memory, for passive

RFID tags types that are written only once and read many times. In the case of write and read many times RFID tags, the encoder (that is 2-19, 2-18 and 2-16) can be implemented in the tag, or the reader can pre-encode the desired stored information when writing into the tag. When the information is retrieved from the tag, that is when the reader reads the tag, the RFID tag transmits the stored information through channel 2-10 back to the reader. The coding gain is realized in this case by virtue of the structure of the stored information in the tag.

[0057] In addition, the SISO decoder may jointly estimate the state of the channel, random phase modeled as a complex multiplier in combiner 2-24. Timing offset, inherently present in any receiver subsystem and particularly in wireless systems, may be modeled in timing offset 2-26, with multi-path propagation characteristics. For channel model 2-22, a finite state machine may be used to represent the channel with memory as shown in channel matrix in equation (3).

[0058] Referring now to Fig. 3, a SISO decoder such as SISO decoder 3-2 can be viewed as a four port device. The input to the SISO decoder 3-2 is the joint probability of channel output 3-10 and transmitted symbol sequence 3-8. The output of SISO decoder 3-2 is the joint probability of channel output 3-4 and transmitted symbol sequence 3-6. The input symbol $\mathbf{a} = (a_k)$ with $k \in \mathbb{N}$ ($\mathbb{N}$ is the set of integers) drawn from a finite alphabet

$A = \{\tilde{a}_1, \tilde{a}_2, \dots, \tilde{a}_N\}$ with a-priori probability $\Pr(\mathbf{a})$. Let $\mathbf{c} = (c_k)$ and $k \in \mathbb{N}$ is the sequence of output drawn from alphabet $C = \{\tilde{c}_1, \tilde{c}_2, \dots, \tilde{c}_N\}$ with a priori probability $\Pr(\mathbf{c})$. The SISO decoder 3-2 accepts at the input the sequence of probability distributions and outputs the sequences of probability distributions, namely: the input probabilities $P_k(a; I)$ in 3-8, $P_k(c; I)$ 3-8 3-10 and output probabilities $P_k(a; O)$ 3-6, $P_k(c; O)$ 3-4.

[0059] Referring now to Fig. 4, a SISO decoder 4-2 is illustrated for use when the proposed channel coding scheme is employed. The input to SISO decoder 4-2 is fed by computing equation (8), shown as the input to the de-interleaver 4-6. Input values of the De-interleaver 4-6 and the output of the interleaver 4-4 are the computed values from the last decoding iteration of the SISO decoder. The soft metric calculation may be performed by computing equation (7) in soft metric calculator 4-8 using the observed signal 4-9 and for a fixed phase value, timing and the channel state from step 4-10. The function and structure of the interleaver 4-4 and de-interleaver 4-6 is dictated by the repetition rate of the outer code

and discussed below. At the end of each iteration the SISO decoder 4-2 outputs $\Lambda_2(\alpha_n)$ s multiple outputs which may then be subtracted from the output of 4-6 and fed to the interleaver block 4-4 to compute the input metric for the next iteration, used in 4-10 and 4-8. This process may be repeated until the SISO decoder 4-2 converges, at which time the extrinsic information is output for decoding the output stream.

[0060] Recursive computation of these input and output joint probability distribution functions, namely: $P_k(\alpha; I)$, $P_k(\alpha; 0)$, $P_k(c; 0)$ and $P_k(c; I)$ may be made possible by modeling the received symbols as output from a discrete-time finite-state Markov process source. The state of the source at time t is denoted by S_θ^t , and its output by Y . A state sequence of the source extending from time t to t' is made possible based on the underlying finite state machine model. The corresponding output forms a first order Markov chain, i.e.

$$\Pr(S_\theta^{t+1} | S_\theta^t, S_\theta^{t-1}, \dots, S_\theta^1) = \Pr(S_\theta^{t+1} | S_\theta^t) \quad (9)$$

[0061] Referring now to Fig. 5, for the purpose of phase sequence estimation and open loop tracking, the phase space may be quantized into Q^ϕ equally spaced intervals and denoted as:

$$\Theta^\phi = \left\{ 0, \frac{\pi}{M}, \frac{2\pi}{M}, \dots, \frac{(M-1)2\pi}{M} \right\} \quad (10)$$

[0062] The phase sequence can be modeled as a random walk around the unit circle, that is a Markov process: $\phi_n = \phi_{n-1} + \Delta\phi \bmod 2\pi$, where $\phi_n \in \Theta^\phi$ and $\Delta\phi$ can be modeled as discrete random variable taking values in the quantized phase space from a known probability density function (i.e. quantized Gaussian, Tikhonov or etc.). The probability of such a phase transition may be denoted as p_{ij} .

[0063] The M distinct states of the Markov source are indexed by the integer m , $m = 0, 1, \dots, (M-1)$ with probability transition matrix:

$$\mathbf{P} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1M} \\ p_{21} & p_{22} & & \vdots \\ \vdots & & \ddots & \\ p_{M1} & p_{M2} & & p_{MM} \end{pmatrix} \quad (11)$$

Where $\sum_{i=1}^M p_{ij} = 1$ and $p_{ij} = p_{ji}$, i.e. matrix is symmetric and doubly Markov.

[0064] Referring now to Fig. 6, the symbol duration Q^r may be quantized into equally spaced intervals for time and synchronization. The timing space may be represented as:

$$\Theta^r = \{\tau, \pm 2\tau, \pm 3\tau, \dots\} \quad (12)$$

Let: $\Upsilon = \left\{ \bigcup_{i=1}^V (t \in [nT_{sym} \pm i\tau, (n+1)T_{sym} \pm (i+1)\tau]) \right\}$ represent the ensemble of all possible symbol

timing intervals where V is the cardinality of the set of i such that

$$|nT_{sym} \pm i\tau| < \frac{(nT_{sym} - (n+1)T_{sym})}{2}. \text{ Then } J \text{ represents any member of set } \Upsilon, \text{ i.e. } J \in \Upsilon.$$

[0065] For assigning the transition probability matrix $\mathbf{P}$ for phase tracking, it is possible to use the classical theory of phased-lock-loops where distribution of state phase error and clock stability from the oscillator can be computed or estimated. Thus matrix $\mathbf{P}$ and can be pre-computed based on a single transition probability from one timing state to another. For assigning the transition probability matrix $\mathbf{P}$ for symbol timing, a geometric distribution can

also be used (i.e. $\frac{\partial}{M^n}$ where ∂ is a constant such that $\sum_{n=1}^M \frac{\partial}{M^n} = 1$).

[0066] Assuming the channel impulse response length of L , at each time instance $k = 1, 2, \dots, N$ the state of the channel is a random variable with the property of the memory present in the system that, given Sk , the state $Sk+1$ can only assume one of two values corresponding to a +1 or -1 being fed into the tapped delay line at time k . Thus, given a binary input alphabet $\{+1, -1\}$ the channel can be in one of 2^L states ri , $i = 1, 2, \dots, 2^L$; corresponding to the $2^L 2L$ different possible contents of the delay elements. This set may be denoted by Θ^h the set

of possible states. Additionally, let Θ^e represent the set of possible states of modulation encoder or line encoder or differential encoder.

[0067] Let the product space

$$\Omega = \Theta^e \otimes \Theta^h \otimes \Theta^r \otimes \Theta^h \quad (13)$$

represent the space of all possible states of the system, where $\otimes$ denotes the Cartesian product and N the cardinality of Ω .

[0068] Referring now to Fig. 7, the possible evolution of states $S^n \in \Omega$ can thus be described in form of a trellis diagram. An example of such a trellis structure for a 16-state trellis diagram is illustrated in Fig. 7, where there are 16 transitions from each state of the trellis to the other.

[0069] The state transitions of the Markov source are governed by the transition probabilities. In which case for the forward and backward log probabilities of the SISO decoder may be defined as follows:

$$\begin{aligned} \alpha_k(S) &= \underset{e: S^n(e) \in \Omega}{\text{Max}} \left\{ \alpha_{k-1}(S^s(e)) + \Pi_k(a(e); I) + \right. \\ &\quad \left. \Pi_k(c(e); I) + \Pi_k(c(e); O) \right\} \\ \beta_k(S) &= \underset{e: S^n(e) \in \Omega}{\text{Max}} \left\{ \beta_{k-1}(S^E(e)) + \Pi_{k+1}(a(e); I) + \right. \\ &\quad \left. \Pi_{k+1}(c(e); I) + \Pi_k(c(e); O) \right\} \end{aligned} \quad (14)$$

$\forall k = 1, \dots, N$, where

$$\begin{aligned} \Pi_k(c; I) &\square \log(P_k(c; I)), \quad \Pi_k(a; I) \square \log(P_k(a; I)) \\ \Pi_k(c; O) &\square \log(P_k(c; O)), \quad \Pi_k(a; O) \square \log(P_k(a; O)) \end{aligned} \quad (15)$$

[0070] This maximization is over all the edges e connected to a state selected from the ensemble of all possible states connected in the trellis. Equation (14) in log domain can be represented as:

$$\begin{aligned}
\Pi_k(c;0) &= \underset{e:\alpha(e)=c}{\text{Max}} \left\{ \alpha_{k-1}(S^s(e)) + \Pi_k(\alpha(e);1) + \right. \\
&\quad \left. \beta_k(S^E(e)) \right\} + h_c \\
\Pi_k(\alpha;0) &= \underset{e:\alpha(e)=\alpha}{\text{Max}} \left\{ \alpha_{k-1}(S^s(e)) + \Pi_k(\alpha(e);1) + \right. \\
&\quad \left. \beta_k(S^E(e)) \right\} + h_u
\end{aligned} \tag{16}$$

and initial values

$$\alpha_0(S) = \begin{cases} 0 & s = S_0 \\ -\infty & \text{Otherwise} \end{cases}, \quad \beta_n(S) = \begin{cases} 0 & s = S_n \\ -\infty & \text{Otherwise} \end{cases} \tag{17}$$

[0071] The quantities h_c and h_u are normalization constants to limit the range of the numerical values of α and β . The set of states $\Xi = \{S_1, S_2, \dots, S_n\}$ and edges $E = \{e_1, e_2, \dots, e_k\}$ represent all possible transitions between the trellis states. $S^s(e)$ denotes all the starting states for the transition $e \in E$ to the ending state $S^E(e)$ with input symbol $\alpha(e)$ corresponding to the output symbol $c(e)$.

[0072] Referring now to Fig. 8a, the operation for computation of α_k and β_k for the binary case is illustrated in Fig. 8a, i.e. two transitions to traverse from state S_k to S_{k+1} . In each iteration, the forward and backward log probabilities may be computed by considering the Trellis structure in Fig. 8a, that is

$$\begin{aligned}
\alpha_k &= \max(\alpha_i + m_{ik}, \alpha_j + m_{jk}) \\
\beta_i &= \max(\beta_k + m_{ik}, \beta_l + m_{il})
\end{aligned} \tag{18}$$

[0073] In order to compute the extrinsic information for each bit as shown in Fig. 8b, the input bit sequence may simply be written as:

$$\Pi_k(\alpha;0) = \underset{\substack{\text{All edges} \\ \rightarrow a=1}}{\text{Max}} \{ \alpha + m + \beta \} - \underset{\substack{\text{All edges} \\ \rightarrow a=0}}{\text{Max}} \{ \alpha + m + \beta \} \tag{19}$$

and the extrinsic for the output code is:

$$\Pi_k(c;0) = \underset{\substack{\text{All edges} \\ \rightarrow c=1}}{\text{Max}} \{ \alpha + m + \beta \} - \underset{\substack{\text{All edges} \\ \rightarrow c=0}}{\text{Max}} \{ \alpha + m + \beta \} \tag{20}$$

The branch metric m is computed as:

$$m = \left(\frac{a\Pi(a; I) + c_1\Pi(c_1; I) + \dots + c_r\Pi(c_r; I) +}{\Pi(c_1; \phi) + \Pi(c_1; \tau)} \right) \quad (21)$$

where r represents the index to the selected element of channel symbol output of c .

[0074] This establishes the equivalency of the SISO decoder as shown in Fig. 3 and computation of equations (18) through (21).

[0075] Referring now to Fig. 9a, the structure of Single Parity Check (SPC) code is given. The input stream of size M is de-multiplexed in demux 9-6 into blocks of N subsequences of length M/N . Each subsequences optionally are permuted with N interleavers each of size M/N prior to entering MUX 9-8. These “optional” interleavers (e.g., tags) together with interleavers prior to single parity check code can be used to provide security for RFID system. This method provides a highly secure RFID system. The N data subsequences as described before are repeated q times and permuted with Nq interleavers. The output of the interleaved blocks are all exclusive OR’ed together in combiner 9-10 to form a single parity check sequence of length M/N which is multiplexed in MUX 9-2 to form a serial output stream. The outputs of multiplexer 9-2 are then fed into the modulation encoder 9-4 (which may be FM0 or Miller code). The interleaver blocks 9-8 in this figure each are designed to preserve the Hamming weight of the input vector at the output of interleaver. The repetition q and the code rate defined in this case as $N/(N+1)$ are design parameters chosen for desired length of the output sequence and coding gain. Presently RFID tag identifiers range anywhere from 24-bits to 2048-bits vectors, that is the output block size of the encoder. The input data U , the input to de-multiplexer 9-6, once encoded forms a vector of length $M+M/N$.

[0076] Referring now to Fig. 9b, the structure of Single Parity Check (SPC) decoder is illustrated as an RFID channel SIS) Decoder. The soft output stream of size $M+M/N$ from SISO modulation decoder is de-multiplexed in demux 9b-6 into blocks of $N+1$ subsequences of length M/N . The first N subsequences deinterleaved through the “optional” N deinterleavers each of size M/N which were used to provide security for RFID system. Knowing these permutation represent secure keys for RFID system, the N soft data subsequences after the “optional” deinterleavers may be repeated q times and permuted with Nq interleavers. The output of the interleaved blocks are all collected together with soft outputs from DEMUX 9b-2b for parity bits enter to the SISO single parity check decoder in

SISO decoder 9b-10 to generate soft outputs. The $N+1$ soft output subsequences from SISO single parity check decoder each of length M/N enters N_q deinterleavers 9b-8b. The soft output of deinterleavers enters the SISO repetition decoder. The output of the repetition decoder enters the “optional” interleavers. The output of the “optional” interleaver, together with soft output for parity bits from SISO SPC, are multiplexed in MUX 9b-2b to form a serial output stream. The outputs of multiplexer 9b-2b are then fed into the SISO modulation decoder 9b-4 (e.g. FM0 or Miller decoder). This process goes through several iterations. The output and input of SISO for repetition decoder are summed to provide reliability for input subsequences data streams. The N subsequence streams are input to de-multiplexer 9b-6. The output of the demultiplexed processes are input to hard decision device 9-16 to generate decoded bit stream U . The detailed operation of SISO decoder for repetition code is shown in Fig. 9c in steps 9c-10, 9c-12, 9c-14, 9c-16 and 9c-18. The detailed operation of SISO decoder for SPC is shown in Fig. 9d in steps 9d-10, 9d-12, 9d-14 and 9d-16.

[0077] Referring now to Fig. 10, coherent SISO receiver 10-10 is disclosed. In this case the extrinsic and intrinsic and branch metrics respectively are represented by the set of equations in equations (18) to (21). Callouts indicate the function of each processing subsystem, the analyzer and equalizer block diagram is shown in 10-6, the estimation block in 10-2 and the detector in 10-4. The input signal may have traversed airspace or a wired infrastructure to reach the receiver, there is no limitation in terms of the transport mechanism into the system. The received signal is de-multiplexed into a parallel stream into a size of the packet or frame used in the communication system. The received signal is then fed to the channel equalizer and interference canceller filter bank in input 10-8. This signal is the rotated via a vector phase rotation (vector complex multiplication) 10-10. The output of 10-10 is used to compute the soft metric values which then feeds the SISO decoder 10-14.

[0078] The theory of operation of a coherent SISO decoder may be described as follows: the observed vector 10-50 y is obtained from serial to parallel conversion 10-52 of the received signal to form the vector 10-50. The size M indicated in 10-50 is chosen as the length of the samples in the received packet, or for practical consideration, a convenient length for the desired hardware complexity. The signal 10-50 is fed to channel equalizer 10-16 which is composed of a modulated filter bank. The filter bank transfer function is selected for typical deployment scenario to match the propagation environment and use case scenario. The signal

from channel equalizer 10-16 is rotated in phase by rotator 10-10 and fed into the correlator and soft metric estimation block 10-12. When channel coding is used, the output of estimation block 10-12 is subtracted from the output of the interleaver as discussed above with regard to Fig. 4 and processing in blocks 4-6 and 4-4. The de-interleaver 10-24 and interleaver block 10-26 are matched to the channel encoder interleaver block used for encoding the data in 9-8, when an optional mode when used. The signal from the de-interleaver 10-24 is fed into the SISO receiver 10-14. After each iteration, the output of the SISO decoder 10-14 is input to the interleaver 10-26 whose output is fed into the channel estimation block 10-36 and to the metric computation block 10-12. The channel estimation block 10-36 decodes the channel impulse response in equation (3) and is used to update the filter bank coefficients in the channel equalizer and interference excision block 10-16. The received vector y 10-50 (also denoted as Y_k where the index k denotes the iteration index in 10-30) is also fed into clocks 10-34, 10-28, 10-39 and 10-37. In delay 10-34, the signal is delayed to match the latency required by each iteration as the input data for the channel estimation block. In 10-37 the observed vector is used to detect the preamble sequence and initialize the symbol timing block 10-39. The symbol timing block 10-39 is updated in each iteration from 10-62 which is the same signal as 10-60, which is the output of the SISO decoder. The output of the symbol timing block 10-39 produces a square wave output 10-35 which is used a reference symbol clock source throughout the system. If there is a residual carrier in the waveform, as in some RFID standards, tracking loop 10-46 is used to extract the CW and compute the phase offset from the ideal carrier frequency in carrier offset block 10-38. If a subcarrier is used, as in some RFID standards, the output of carrier offset block 10-38 is further enhanced by estimating an additional phase offset term from the subcarrier phase, by performing fine frequency tracking in 10-42 and by computing the phase offset in phase offset block 10-44. The frequency estimate from fine frequency block 10-42 may also be fed back to FFT 10-18 to update the spectral estimate of the signal for the next iteration.

[0079] In an optional mode, it may be desirable to additionally also perform frequency domain equalization in each iteration of the SISO decoder as shown in detector 10-4. This functionality may be enabled in the presence of fast frequency fading channels in which the signal may suffer fast fades during a single symbol interval. In an RFID system, these may be

caused by conveyor belts, fast moving tunnel highways or moving vehicles. In this case the estimated impulse response state may be fed to the equalizer coefficient estimation block that feeds the FFT block to compensate for fading and multipath effects.

[0080] Referring now to Fig. 11, non-coherent SISO receiver 11-10 is disclosed. The operation of all the computational blocks, namely, 11-18, 11-20, 11-22, 11-16, 11-10, 11-46, 11-44, 11-42, 11-40, 11-38, 11-36, 11-34, 11-37, 11-39, 11-54, 11-46, 11-40, 11-60, 11-62, are the same as in 10-18, 10-20, 10-22, 10-16, 10-10, 10-46, 10-44, 10-42, 10-40, 10-38, 10-36, 10-34, 10-62, 10-37 and 10-39. The channel equalizer and interference canceller 11-16 is similar to the coherent block 10-16, except the input channel estimates may now be based on the non-coherent estimation block for which the equations are presented below. The key distinction between the coherent and non-coherent versions of the receiver architecture is in the computation of extrinsic information for branch metric computation, and the amount of phase rotation imposed in phase rotator 11-10. The channel equalizer block 11-16 is similar to the coherent case with the exception that estimates for the channel coefficients are derived from the non-coherent SISO detector. The SISO decoder 11-14 uses a similar trellis to that of the coherent case, except the branch metrics computed in 11-12 are based on non-coherent signal detection theory which is essentially phase invariant in presence of random or unknown phase. In each iteration in block 11-12, equation (33) is computed and/or updated based on the previous iteration of the extrinsic information, that is the output from the SISO decoder's last iteration via equation (21).

[0081] In a non-coherent case, the received signal (in absence of multipath the symbol c_k is denoted simply by x_k) may be modeled with random or unknown phase as:

$$\mathbf{y}_k = A\mathbf{x}_k e^{j\phi} + \mathbf{n}_k \quad (22)$$

[0082] In an AWGN channel with n_k , that is complex zero mean Gaussian noise with variance σ^2 per dimension, the observed vector's probability distribution function conditioned on a known phase and the transmitted sequence of N symbols is:

$$P(\mathbf{y}|\mathbf{x}, \phi) = o \cdot e^{-\frac{1}{\sigma^2} \sum_{n=1}^N |y_n - Ax_n e^{j\phi}|^2} \quad (23)$$

Where o is a constant and σ is the variance of the noise. After some algebraic manipulation we can write (23) as

$$P(\mathbf{y}|\mathbf{x}, \phi) = o. e^{-\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2} e^{\frac{A}{\sigma^2} \operatorname{Re} \left(\sum_{n=1}^N y_n^* x_n e^{j\phi} \right)} \quad (24)$$

Averaging (24) over the uniformly distributed phase over $(0, 2\pi)$ yields:

$$P(\mathbf{y}|\mathbf{x}) = o'. e^{-\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2} I_0 \left(\frac{A}{\sigma^2} \left| \sum_{n=1}^N y_n^* x_n \right| \right) \quad (25)$$

where $I_0(\cdot)$ represents the modified zero-th order Bessel function.

Recall

$$P(x_i = x|\mathbf{y}) = \frac{1}{P(\mathbf{y})} \sum_{\mathbf{x}: x_i = x} P(\mathbf{y}|\mathbf{x}) \prod_l P(\mathbf{x}) \quad (26)$$

From (25),

$$\frac{P(x_i = x|\mathbf{y})}{P(x_i = x)} = o'. \sum_{\mathbf{x}: x_i = x} \left(e^{-\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2} \times I_0 \left(\frac{A}{\sigma^2} \left| \sum_{n=1}^N y_n^* x_n \right| \right) \right) \prod_{l \neq i} P(x_l) \quad (27)$$

Or equivalently, the extrinsic metric may be approximated in equation (27) as

$$\prod_l (x_l = x, 0) \approx \max_{\mathbf{x}: x_i = x} \left\{ \begin{aligned} & -\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2 + \\ & \frac{A}{\sigma^2} \left| \sum_{n=1}^N y_n^* x_n \right| + \\ & \sum_{l \neq i} \ln p(x_l) \end{aligned} \right\} \quad (28)$$

For the special case when x_n takes values +1 and -1, then the term $-\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2$ can be ignored, since $|x_n|$ is constant.

[0083] Next consider a Rayleigh fading channel model, where in equation (22), the magnitude A is Rayleigh distributed and the phase is uniformly distributed over $(0, 2\pi)$ interval. The observed vector's probability distribution function conditioned on a known amplitude and the transmitted sequence of symbols is:

$$P(\mathbf{y}|\mathbf{x}, \mathbf{A}) = \propto e^{-\frac{1}{2\sigma^2} \sum_{n=1}^N |y_n|^2} e^{-\frac{A^2}{2\sigma^2} \sum_{n=1}^N |x_n|^2} e^{\frac{2}{2\sigma^2} \text{Re} \left(\sum_{n=1}^N y_n^* x_n \right)} \quad (29)$$

Lets assume that the average power of A is σ_f^2 and taking the expectation with respect to complex random variable A results in $P(\mathbf{y}|\mathbf{x}) = E_A \{P(\mathbf{y}|\mathbf{x}, A)\}$.

$$P(\mathbf{y} \mid \mathbf{x}) = \iint_{\mathcal{O}} e^{-\frac{1}{2} \left[\frac{\sum_{n=1}^N |x_n|^2}{\sigma^2} + \frac{1}{\sigma_f^2} |A|^2 + \frac{2}{\sigma^2} \operatorname{Re} \left(\sum_{n=1}^N y_n^* x_n \right) \right]} dA \quad (30)$$

which can be integrated to:

$$P(\mathbf{y} \mid \mathbf{x}) = c'' \frac{1}{\left[\frac{\sum_{n=1}^N |x_n|^2}{\sigma^2} + \frac{1}{\sigma_f^2} \right]} e^{-\frac{1}{2} \left[\frac{1}{\sigma^2} \sum_{n=1}^N y_n^* x_n \right]^2} \quad (31)$$

For obtaining the extrinsic information, from equation (31), the following equation applies

$$\begin{aligned}
 & \frac{P(x_i = x | \mathbf{y})}{P(x_i = x)} = \\
 & c'' \sum_{\mathbf{x}: x_i = x} \left[\frac{1}{\frac{\sum_{n=1}^N |x_n|^2}{\sigma^2} + \frac{1}{\sigma_f^2}} \right] e^{-\frac{1}{2} \left| \frac{1}{\sigma^2} \sum_{n=1}^N y_n^* x_n \right|^2} \prod_{l \neq i} P(x_l) \quad (32)
 \end{aligned}$$

which after some algebraic manipulation can be simplified to:

$$\prod_i(x_i, 0) = \text{Max}_{\mathbf{x}: x_i = x} \left\{ \frac{1}{2} \left[-\ln \left[\frac{\sum_{n=1}^N |x_n|^2}{\sigma^2} + \frac{1}{\sigma_f^2} \right] + \frac{\frac{1}{2} \left| \frac{1}{\sigma^2} \sum_{n=1}^N y_n^* x_n \right|^2}{\sum_{n=1}^N |x_n|^2 + \frac{1}{\sigma_f^2}} \right] + \sum_{l \neq i} \ln P(x_l) \right\} \quad (33)$$

It should be noted that $\prod_i(x_i, 0)$ is defined as $\ln p(x_i)$

[0084] Referring now to Fig.s 12a and 12b, and in particular Fig. 12b, the operation of an iterative cascaded SISO receiver, with non-coherent and coherent models as described earlier, may be as follows:

[0085] Received vector $\mathbf{y}_k$ may be initially iterated in the non-coherent SISO receiver until the stopping rule for minimizing the sequence error probability is satisfied. The output of the non-coherent receiver for the estimated symbol sequence, timing, phase and channel response may then used for the initial estimate of these sequences in the subsequent coherent SISO receiver. The SISO decoder of 12-14 and 12-2 are essentially same decoders, except the SISO decoder 12-12 receives its input branch metrics from extrinsic information from the non-coherent SISO decoder 12-6.

[0086] Coherent SISO receiver system 12-10 is shown in Fig. 12a in which a received signal is applied to branch metric generator 12-12 which computes the branch metric m_{ik} in equation (18). These branch metrics are computed for each transition for each state of the trellis from one-to-the-other. The branch metrics are input to coherent SISO decoder 12-14. After a sufficient number of iterations (indicated by loop 12-16) in effect minimizing the sequence error probability in each iteration, the decoder slightly improves and reduces the

error probability. The switch 12-18 may driven by a fixed or dynamic rule. Typically after five to ten iterations, the SISO decoder output can be sampled and hard quantized. An alternative approach would be to monitor the dynamic range of the extrinsic values and when the values reach steady state (no longer changing or arbitrarily small change), the SISO decoder may be stopped and the output may be hard limited in block 12-20 and decoded .

[0087] Referring now to Fig. 12b, cascaded non-coherent and coherent SISO receiver system 12-22 is depicted in which the received signal is used by the branch metric generator 12-8 to output the metric values to the non-coherent SISO decoder 12-6. The difference between 12-2 and 12-8 is that the branch metric values for the non-coherent case are computed by considering the distribution of phase to be random, where in the coherent case the phase is assumed to be known . After a sufficient number of iterations (as shown by loop 12-24), the output of the non-coherent SISO decoder 12-6 is sampled by sample switch 12-26 and applied to coherent SISO decoder 12-12. After a sufficient number of iterations (as shown by sample loop 12-28), the output is applied by sample switch 12-30 to hard limiter 12-4 and then provided to the data user which in RFID application is the protocol layer-2 embedded in the reader system. An option for the stopping rule to close the switches 12-26, 12-28 and 12-30 is to monitor the rate of growth of the accumulated forward and backward metrics in equation (14) in each SISO decoder, and then stop the iteration when the difference between successive iterations is arbitrarily small for all the states in the Trellis.

[0088] Referring now to Fig. 13a, an implementation of RFID system 13-10 is shown in which plurality of inventory items, such as items 13-7, each of which may include a passive RFID tags 13-6. The reader/interrogator 13-1 emanates a signal to RFID tags 13-6 to respond with their respective identification code referred to as "electronic product codes" (EPC). The RFID tags 13-6 subsequently respond to signals generated by reader 13-1 by backscattering the received signal with their respective EPCs. The signal may be corrupted by multipath 13-4 from the flooring the walls and moving and fixed obstacles 13-8.

[0089] Referring now to Fig. 13b, reader/interrogator 13-1 includes transmitter-antenna subsystem 13-24 which is modulated by data from data source system 13-36 applied to modulation encoder 13-15 and transmits encoded RF signals to RFID tags 13-7. Alternatively, outer coder 13-28, interleaver 13-48 and/or single parity coder 13-50 may be inserted between data source 13-36 and encoder 13-52 in appropriate implementations.

[0090] Reader interrogator 13-1 also includes receiver 13-28 which receives reflected signals from RFID tags 7 and applies them to receiver system 13-30 for detection and decoding. The output of receiver system 13-30 provides data to a system user. Various obstacles, including sources of interference and multi-path reflection such as stationary and moving objects 13-8 may be in the path of the transmitted and/or received signals.

[0091] System 13-10 may, for example, be deployed in a department store in which items in cases of items with RFID tags 13-6 are displayed for sale. Moving and stationary objects 13-8 may represent shoppers and store personnel moving during the day across the transmission and reception paths as well as relatively stationary objects such as one or more potential reflectors, e.g. including advertising displays or other racks of may be moved or changed on a less frequent basis. System 13-10 may be deployed in order to keep track of inventory items, for example, to detect and prevent attempted shoplifting and/or for other reasons related to inventory control by providing data from reader interrogator 13-1 to a user.

[0092] Data source system 13-12 includes data source 13-36 which provides a command or an EPC to the RFID tag 13-7. Channel coding techniques may be used to improve the overall system performance. In the event channel coding is employed, the electronic product code stored in RFID tag 7 is used as the input. The data source may embed the Electronic Product Code (EPC) in pre-coded format by using outer coder 13-38, interleaver 13-48 and single parity coder 13-50 at the time that the stored data is written into the RFID tag. In that event, the model of data source 13-36 simplifies to a table look-up for EPC which, in the case of passive RFID tags, is backscattered (or transmitted) to the interrogator or the RFID reader. It is also noted that it is possible to compress the EPC code in the interrogator prior to application of channel coding, using simple hashing method to decrease the length of the information sequence. Thus, the additional storage in the RFID tag is used to store the resulting parity bits. For example, for a 32-bit EPC code, the sequence can be hashed into a 16-bit code by the interrogator in which case the effective coding rate would be rate one-half, and the remaining 16-bit is used as a parity check sequence. The channel coding method may be used for protection against channel error. The code shown in Fig. 9 is a repetition code in which each data bit is repeated with a fixed number of multiplicity. The number of repetitions of each input bit is a design parameter which determines the overall coding rate of the system. The interleaver 13-48 serves to permutate the encoded data from the outer code output 13-38,

such that the Hamming distance of the input sequence is preserved and the output is applied to single parity coder 13-50 and described earlier in Fig. 9. The output of which is applied to modulation encoder 13-52. The modulator may use various modulation techniques and waveforms defined by various RFID tag or sensory standardization bodies. System 13-10 is applicable to any modulation technique or waveform. That is, modulation encoder 13-52 can be amplitude shift keying (ASK), on-off keying (OOK), frequency modulation (FM) and other modulation schemes without any loss of generality in applying the receiver subsystem in 13-30.

[0093] RFID tags 13-7 operate to backscatter or actively transmit the embedded information sequence to the reader or the interrogator to produce the signals received in equation (2). Stationary and moving obstacles 13-8 may cause interference between the signals reflected by one or more of the RFID tags 13-7. The signals received by receiver 13-30 may therefore include channel interference, multi-path reflections and other effects which make detection and discrimination between RFID tags 13-7 difficult with very low signal levels. Additional anomalies may also be present in the communication channel. In an in-door environment such as warehouses, factories and malls substantial scattering due to multipath and man-made interference (e.g. drill noise, cordless phones) or natural interferences (e.g. ceiling lighting) may also be present. In an outdoor environment interference and multipath effects may also be present in addition to signal blockage due to foliage and weather effects due to humidity or rain. These channel anomalies and interferences may all be handled by receiver system 13-30.

[0094] Receiver system 13-30 serves to detect and discriminate between RFID tags 13-7 by taking advantage of SISO decoding proposed herein. It is assumed that latency in SISO decoding can be tolerated by the users of the system 13-10 or the processing time in system 13-10 is short for real or near real time detection of motion of individual RFID 13-7. That is, reader/interrogator 13-1 processes the signals received by receiver system 13-30 for a relatively long time and is able to distinguish between transmission channels from different RFID tags by learning the signal characteristics. Furthermore, in warehouse, factory and airport deployment scenarios the RFID tags may be moving at high velocity on conveyor belts or moving vehicles while being manipulated. Reader Interrogator 13-1 also compensates for effect of moving RFID tags on the characteristic of the received signal. That is the system 13-

10 can tolerate a high level of Doppler shift and still achieve high performance in detection of signals from RFID tags.

[0095] Receiver system 13-30 also provides a frequency signal to receiver 13-28 to adjust the transmitted frequency. This frequency adjustment provides a mechanism to both track and adopt the frequency channel used to read and write information into the RFID tag and also support optional waveforms which employ frequency hopping techniques as defined by RFID Standardization Bodies (e.g. ISO, EPC Global).

[0096] Receiver system 13-30 processes the received signals in channel equalizer and interference canceller 13-54 which is realized by a bank of adaptive linear phase filter banks with the objective of maximizing the received signal power and minimizing the effect of interference by excision. That is, the frequency response of the filter bank is designed to eliminate narrow band interference while maximizing the signal-to-noise ratios received from the RFID tag. The output of channel equalizer and interference canceller 13-56 is applied to rotator 13-58 which appropriately adjust the phase of the incoming signal in real-time to track the phase of the incoming signal and compensate for the effect of motion, Doppler and phase noise due to imperfection in the environment.

[0097] The output of rotator 13-56 is applied to SISO processor 13-58, which includes SISO decoder 13-60, and which serves to input into the soft metric calculator which calculates the intrinsic metric values associated with each transition from one state of trellis structure to the other state (or Bi-partite graph). The output of SISO processor 13-58 is applied to phase, channel and frequency estimator 13-62 which serves to provide an instantaneous phase and frequency estimate of the received signal based on the output of the SISO decoder.

[0098] One output of phase, channel and frequency estimator 13-62 is applied to rotator 13-56 and provides the reference for phase compensation of the received signal which may have been caused by motion or other anomalies. A second output of phase, channel and frequency estimator 13-62 is applied to channel equalizer and interference canceller 13-54 and provides the adaptation algorithm with the phase and frequency of variables used to compute the channel equalizer and interference canceller coefficients of the Finite Impulse Response Filter.

[0099] The output of user system 13-34 is formed by summing the extrinsic and intrinsic information and then hard quantizing the resulting sum. This value constitutes the detected bit

stream from the RFID tag. SISO decoder 13-60 in SISO processor 13-58 also includes soft metrics calculator 13-66, de-interleaver 13-64 and interleaver 13-67 when channel coding as discussed earlier is employed.

[00100] In operation of system 13-30, both fine and coarse motion of items 13-6 having RFID tags 13-6 can be accurately detected and observed because the SISO decoder in 13-60 simultaneously estimates the channel response, symbol timing and effectively performs open loop phase tracking.

[00101] Referring now to Figs. 14a and 14b, the FM0 and Miller codes can also be used in passive RFID applications. In FM0 encoder 1410, user data 14-22 is provided to x-or gate 14-18 the output of which is provided to bit mapper 14-16 as well as to simple delay circuit 14-23. The output of delay 14-23 may be provided as a second input to x-or gate 14-18 as well as to inverter 14-20, the output of which is applied to bit mapper 14-14. The two sequences from bit mappers 14-14 and 14-16 are respectively multiplexed into a single stream in multiplexer 14-12 and each repeated once in repeater 14-21 to provide output data 14-24 which is the FM0 encoded data for use by the modulator. FMO encoder 1410 may be used as a data source, such as data source 2-2 in Fig. 2 or data source 2-20 in Fig. 2b.

[00102] In Miller encoder 14-60, delay taps 14-44 and 14-36 are used. The combinatorial logic consists of three inverters 14-46, 14-50, 14-52, two or-gates 14-32 and 14-34, and three and-gates 14-42, 14-36 and 14-38. The output sequence of the combinatorial and delay logic is fed into the signal mapping blocks 14-56 and 14-58 which is multiplexed in 14-30 and repeated in 14-57 to form the output data 14-48 for Miller encoded data for use by the modulators.

[00103] Referring now to Fig. 15a, the technique for the coherent detection of FM0 or Miller encoded signal is depicted. The system consists of using the channel data 15-28 and integrating the signal over each symbol period during each half a symbol interval in integrate and dump 15-34 and de-multiplexing the real and imaginary part in demux 15-36 and forming the cross product in step 15-38, taking the real part in block 15-42, hard quantizing the output in quantizer 15-44 and mapping the data into ones and zeros from -1/+1 in data block 15-46. This is the coherent case.

[00104] Referring now to Fig. 15b, a similar operation is performed in non-coherent case in blocks 15-30, 15-32, 15-60, 15-62, 15-64 and 15-52 except only the real part of the signal is

used to form the cross product. The output of the non-coherent detector 15-66 and coherent detector is 15-48. N_s denotes the number of sample per symbol, i.e. $N_s = T_{sym} / T_s$ that is the ratio of the symbol time to sampling period.

[00105] Referring now to Fig. 15c, a block diagram of a multiple symbol detector is shown for the non-coherent detection case. Channel data 15-80 is applied to integrate and dump 15-80 and the real part is determined by block 15-76 and demultiplexed in demux 15-74. The output is applied to non-coherent multiple symbol detector 15-70 to provide output 15-72.

[00106] Referring now to Fig. 16, multiple symbol non-coherent detector (MSNNonCoh) for FM0 is disclosed. In this example, the non-coherent detection is done over a particular sequence of half symbol observations which starts from middle of data interval rather than beginning of data interval. In passive RFID systems, the presence of CW translates into having a DC component. The received signal with FM0 encoding at time i in presence of DC component is:

$$\begin{aligned} y_{1,i} &= (x_{1,i} + c)e^{j\phi} + n_{1,i} \\ y_{2,i} &= (x_{2,i} + c)e^{j\phi} + n_{2,i} \end{aligned} \quad i = k - N + 2, \dots, k + 1 \quad (33)$$

where c is a dc component, ϕ is carrier phase offset (or phase noise). Without loss of generality, it can be assumed that the phase error is constant over duration of a symbol and $n_{1,i}$ and $n_{2,i}$ zero mean complex Gaussian samples with variance σ^2 per dimension. First the dc value c at the receiver can be estimated as:

$$\hat{c} = \frac{1}{N} \left(\sum_{i=k-N+2}^{k+1} (y_{2,i-1} + y_{1,i}) \right) \quad (34)$$

The new observation can be defined as

$$\begin{aligned} r_{1,i} &= y_{1,i} - \hat{c} \\ r_{2,i} &= y_{2,i} - \hat{c} \end{aligned} \quad (35)$$

Next the Maximum Likelihood (ML) probability of the modified observation can be computed. The particular observations are:

$$r_{2,k-N+1}, r_{1,k-N+2}, r_{2,k-N+2}, r_{1,k-N+3}, \dots, r_{2,k}, r_{1,k+1}$$

The conditional probability function can be formulated as:

$$P(\mathbf{r} | \mathbf{x}, \phi) = \text{constant } e^{-\frac{1}{2\sigma^2} \sum_{i=k-N+2}^{k+1} \{|r_{2,i-1} - x_{2,i-1}|^2 + |r_{1,i} - x_{1,i}|^2\}} \quad (36)$$

Averaging (36) over the carrier phase, the ML function can be approximated with

$$P(\mathbf{r} | \mathbf{x}) \approx I_o \left(\frac{1}{2\sigma^2} \left| \sum_{i=k-N+2}^{k+1} \{r_{2,i-1}x_{2,i-1} + r_{1,i}x_{1,i}\} \right| \right) \quad (37)$$

Since the zero order modified Bessel function is a monotonic function, thus the required metric for the decision is:

$$\text{Metric} = \left| \sum_{i=k-N+2}^{k+1} (r_{2,i-1}x_{2,i-1} + r_{1,i}x_{1,i}) \right| \quad (38)$$

The key property of FM0 encoder output 14-24 for RFID application is

$$\begin{aligned} x_{2,i} &= d_i x_{2,i-1} \\ x_{1,i} &= -x_{2,i-1} \end{aligned} \quad (39)$$

Replacing (39) in (38) one gets:

$$\text{Metric} = \left| \sum_{i=k-N+2}^{k+1} (r_{2,i-1} - r_{1,i})x_{2,i-1} \right| \quad (40)$$

or

$$(\hat{d}_k, \hat{d}_{k-1}, \dots, \hat{d}_{k-N}) = \arg \max_{d_k, d_{k-1}, \dots, d_{k-N+2}} \left| (r_{2,k-N+1} - r_{1,k-N+2}) + \sum_{i=k-N+3}^{k-1} (r_{2,i-1} - r_{1,i}) \prod_{j=k-N+2}^{i-1} d_j \right| \quad (40a)$$

[00107] By expanding the sum for the case of $N=3$, the optimum decision rule for multiple symbol non coherent detection rule becomes:

$$(d_k, d_{k-1}) = \arg \max_{d_k, d_{k-1}} \left| (r_{2,k-2} - r_{1,k-1})d_{k-1} + (r_{2,k-1} - r_{1,k}) + (r_{2,k} - r_{1,k+1})d_k \right| \quad (41)$$

In step 15-70, equation (41) is realized and the maximization implemented over all possible data symbols $d_k \in \{+1, -1\}$. Note that this metric is independent of dc offset and can be used even without using (39).

[00108] Referring now to Fig. 16, the Trellis diagrams from the encoder structure of Fig. 14 is shown in trellis 16-2 for FM0 and in trellis 16-4 for Miller code. These Trellis diagrams are used for the SISO decoder for application of passive RFID tag standards which employ these encoding techniques. In the presence of random phase and timing, the Trellis diagram may be too large and impractical to be illustrated graphically. That is due to the large number of states and transitions (e.g. 2000 states and 20 transitions per state) which depends on the choice of the cardinality of the sets in equations (10) and (12).

[00109] Referring now to Fig. 17, the performance of detectors in Fig. 15a, 15b and 15c are compared. The theoretical performance of coherent and non-coherent detector over AWGN are also depicted with solid lines and the performance of multiple symbol non-coherent MSNC is simulated and shown by small triangles. It is noted that the performance of the symbol non-coherent detector outperforms the classical non-coherent detector by a factor of 3.5 dB.

[00110] In SISO decoder 4-2 a long sequence, typically a packet or a frame, is processed at a time. Hence, the performance is still even superior to that of symbol non-coherent detection in which the Maximum Likelihood detector is considering only three symbols. In applications for system 13-10 are for RFID tag standards in which the tag protocol is amenable to longer latency which results from the SISO decoding. Typical applications of multiple symbol non-coherent detector 15-70 are when the RFID standard requires very strict timing requirements between the tag-to-reader and reader-to-tag packet inter-arrival time. These tight timings requirements typically occur when acknowledgement or replies are required from the reader to the RFID tag or vice versa. In certain circumstances and for certain RFID tag standards, it is also possible to employ both systems 13-10 and 15-70 so that for certain packets types which the system 15-70 is used and system 13-10 may be used for other timing critical packets. Specifically, when detecting the product code itself from the received packet, SISO decoding in 13-10 may be used, but for other packet types which are short replies and handshake, system 15-70 may be used.

[00111] Referring now to Figs. 18 and 19, a typical problem for many digital communication systems is that the baud rate is fixed, i.e. the transmitted pulse duration is fixed. In sensor networks and RFID systems in particular, the transmitted pulses from the tag can change in duration from symbol to symbol. Thus at the reader's receiver, the duration of pulses or the instantaneous time varying baud rate should be tracked. In order to track timing for such applications, a timing trellis may be used.

[00112] Assume that the time axis is sampled at time instants iT_s , where $1/T_s$ represent the sampling rate. The sampling points at the output of matched filter are depicted by bullets "•" on the time axis in Fig. 19-10. There may be N samples per nominal baud interval. Thus the nominal symbol duration would be $T_s = NT_s$, where T is the nominal symbol duration. Assume the symbol duration from symbol to symbol can increase (as a result for example of changing channel characteristics) by one sample to $T_s = (N+1)T_s$ with probability p , or no change $T_s = NT_s$ with probability $(1-2p)$, or can decrease by one sample to $T_s = (N-1)T_s$ with probability p .

[00113] Each interval has N tick marks that denote possible positions (in multiples of T_s), where a sample can be taken at the output of the matched filter. From Fig. 19, some intervals have one tick mark as depicted in 19-2, 19-3 and 19-4, some intervals have two tick marks, while some intervals have no tick marks as shown in 19-12. Denote the timing state as S_k which its value corresponds to a tick mark. The state is associated with a time interval $((k-1)T, kT]$, and can take one of the values in the following set: $S_k = s_0, s_1, \dots, s_N, s_{N+1}$. State s_0 denotes that the k th symbol interval $((k-1)T, kT]$ is not sampled at all. For example, in Fig. 19, the interval corresponding to $S_k = s_2$ shown in 19-13 is sampled at the second tick from the start of the interval. State $S_k = s_i$, for $1 \leq i \leq N$ denotes that the k th symbol interval $((k-1)T, kT]$ is sampled only once at the i -th tick.

[00114] Referring now also to Fig. 18, state $S_k = s_{N+1}$ (for $N=8$ in Fig. 19) denotes that the k th symbol interval $((k-1)T, kT]$ is sampled twice. The only way an interval can be sampled twice is if it is sampled at the first and N th ticks, since we only allowed maximum of one sample variation from symbol to symbol. The constraints prevent any other way of two samples falling in the same interval. There are some restrictions on how the sampling-states S_k can evolve. To represent all valid sampling-state transitions, we form a timing trellis, depicted in Fig. 18. To a branch in the timing trellis, we associate a transition probability $\Pr(S_k | S_{k-1})$. The transition probabilities can be computed based on parameter p . A key feature of the

timing trellis in Fig. 18 is that the branches in the trellis carry a variable number of samples. We will denote the vector of samples taken in the timing interval $((k-1)T, kT]$ by $\mathbf{r}_k$. Note that $\mathbf{r}_k$ could be an empty vector if no sample is taken in the k th symbol interval.

[00115] The timing trellis has $N+2$ states. The present state S_{k-1} i.e. S_0 through S_9 (18-12) and next states S_k i.e. states S_0 (18-14) through (18-16) are shown in Fig. 18. Let's assume $N=8$ for clarification and rectangular NRZ pulses. For symbols with nominal duration of 8 samples, the matched filter sums the recent 8 samples. To transition from state S_0 to state 1, the matched filter sums nine recent samples and produces observation r_k . To transition from state S_0 to state 9, the matched filter sums nine recent samples and produces observation r_k , and the next seven samples to produce observation r_{k+1} corresponding to data a_k and a_{k+1} respectively. Each state also should store the most recent index of observation sample. The branch metric per edge of trellis requires variable number of samples. Denote the index of observation sample to state S_{k-1} at time $k-1$ by q_i , then the number of samples required to compute the edge branch metric are $q_i + N(s_i, s_j)$ samples. Where $N(s_i, s_j)$ represent the number of samples required to compute the branch metric from present state $S_{k-1} = s_i$ to next state $S_k = s_j$. For $N=8$:

$$\begin{aligned}
 &N(s_0, s_1)=9 \quad N(s_0, s_9)=9+7 \quad N(s_1, s_1)=8 \quad N(s_1, s_2)=9 \quad N(s_1, s_9)=8+7 \\
 &N(s_2, s_1)=7 \quad N(s_2, s_2)=8 \quad N(s_2, s_3)=9 \quad N(s_2, s_9)=7+7 \quad N(s_2+i, s_2+i-1)=7 \text{ for } \\
 &i=1,2,3,4,5 \\
 &N(s_2+i, s_2+i)=8 \text{ for } i=1,2,3,4,5 \quad N(s_2+i, s_2+i+1)=9 \text{ for } i=1,2,3,4,5 \quad N(s_8, s_0)=\text{no samples} \\
 &N(s_8, s_7)=7 \quad N(s_8, s_8)=8 \quad N(s_9, s_0)=\text{no samples} \quad N(s_9, s_7)=7 \quad N(s_9, s_8)=8
 \end{aligned}$$

[00116] Referring now to Fig. 20, a folded timing trellis is similar to the method shown in Figs 18 and 19, except the number states are less and number of transitions per state is fixed number for all timing states. The time axis may be sampled at time instants iT_s , where $1/T_s$ represent the sampling rate. The sampling points at the output of matched filter (end of actual symbol time duration) are depicted by bullets “•” on the time axis in Fig. 19-10. Assume there are N samples per nominal baud interval. Thus the nominal symbol duration is $T_s = NT_s$, where T is the nominal symbol duration. Assume the symbol duration from symbol to symbol can

increase by one sample to $T=(N+1)T_s$ with probability p , or no change $T=NT_s$ with probability $(1-2p)$, or can decrease by one sample to $T=(N-1)T_s$ with probability p .

[00117] Each interval has N tick marks that denote possible positions (in multiples of T_s), where a sample can be taken at the output of the matched filter. The state is associated with a time interval $((k-1)T, kT]$, and can take one of the values in the following set: $S_k = s_1, \dots, s_N$. State $S_k = s_i$, for $1 \leq i \leq N$ denotes that the k th symbol interval $((k-1)T, kT]$ is sampled at the i -th tick from the beginning of the interval. There are some restrictions on how the sampling-states S_k can evolve. To represent all valid sampling-state transitions, a timing trellis may be formed as depicted in Fig. 20. To a branch in the timing trellis, a probability $\Pr(S_k | S_{k-1})$ can be assigned to a transition. The transition probabilities can be computed based on parameter p . A key feature of the timing trellis in Fig. 20 is that the branches in the trellis carry a variable number of samples. The vector of samples taken in the timing interval $((k-1)T, kT]$ can be denoted by r_k .

[00118] The timing trellis has N states. Lets assume $N=8$ for clarification. The present states S_{k-1} i.e. S_1 (20-10) through S_8 (20-12) and next states S_k i.e. states S_1 (20-14) through (20-16) are shown in Fig. 20. Also assume rectangular pulses. For symbols with nominal duration of 8 samples, the matched filter sums the recent 8 samples if there is a transition from present state S_i to the next state S_i for $i=1,2,\dots,N$ (for the example in Fig. 20, $N=8$). For symbols with nominal duration of 8 samples, the matched filter sums the recent 9 samples if there is a transition from present state S_i to the next state S_{i+1} for $i=2,3,\dots,N$, and S_1 to S_8 (for the example in Fig. 20, $N=8$). For symbols with nominal duration of 8 samples, the matched filter sums the recent 7 samples if there is a transition from present state S_i to the next state S_{i-1} for $i=1,2,\dots,N-1$, and from present state S_N to S_1 (for the example in Fig. 20, $N=8$). Each state also should store the most recent index of observation sample to compute the branch metric for the next trellis section. Thus the branch metric per edge of trellis requires variable number of samples. Denote the index of observation sample to state S_{k-1} at time $k-1$ by q_i , then the number of samples required to compute the edge branch metric are $q_i + N(s_i, s_j)$ samples. Where $N(s_i, s_j)$ represent the number of samples required to compute the branch metric from present state $S_{k-1} = s_i$ to next state $S_k = s_j$. For $N=8$:

$$N(s_1, s_2)=7 \quad N(s_1, s_1)=8 \quad N(s_1, s_8)=9$$

$$\begin{aligned}
N(s_i, s_{i-1}) &= 7 \quad \text{for } i=1,2,3,4,5,6,7 \\
N(s_i, s_i) &= 8 \quad \text{for } i=1,2,3,4,5,6,7,8 \\
N(s_i, s_{i+1}) &= 9 \quad \text{for } i=2,3,4,5,6,7,8 \\
N(s_8, s_1) &= 7 \quad N(s_8, s_8) = 8 \quad N(s_8, s_7) = 9
\end{aligned}$$

[00119] Referring now to Fig.s 21 and 22, the symbol timing tree structure is based on a nominal value of N samples per symbol. This means that the granularity of the timing captured will be $\frac{1}{N \times F_s}$ where F_s is the sampling frequency. The rates may be discussed in the $\frac{1}{F_s}$ domain, meaning that rates will be expressed in percentage of the sample rate, and time in samples. To build a structure that can be integrated into the trellis form, an estimate of the first symbol time must be provided that is accurate to one symbol period ($\pm \frac{N}{2}$). If the first symbol time cannot be estimated to this accuracy, a separate synchronization sequence may be required. States are labeled $S_{M,i}$ for the i th state in the M th stage. In the general case, there may be N starting states, labeled from $S_{0,0}$ to $S_{0,N-1}$. Each state $S_{M,i}$ has $2 \times \Delta_{max} + 1$ (where Δ_{max} represents the maximum number of samples from symbol duration can exceed from nominal symbol duration) transitions leading to consecutive states starting at $S_{M+1, i - \Delta_{max}}$ and ending at $S_{M+1, i + \Delta_{max}}$. To further refine the structure, an a-priori estimate of the maximum timing error (expressed in samples per symbol) of R can be used. If N is nominal number of samples per symbol, then $R = rN$ where r is percentage of timing error. The definition of R becomes $\Delta_{max} = \lceil R \rceil$ which is an integer. This limits the states at any given trellis stage M to states starting at $S_{M, 0 - \lfloor R \times M \rfloor}$ up to $S_{M, N-1 + \lceil R \times M \rceil}$ where $\lceil x \rceil$ is the ceiling of x (the next higher integer), and $\lfloor x \rfloor$ is the floor of x (the next lower integer). This means that at any stage M the state $S_{M,i}$ corresponds to a symbol that starts at sample time $M \times N + i$. An example of this structure for $\Delta_{max} = 1$ and $N = 4$ is shown in Fig. 22.

[00120] Referring now to Fig. 23, a second, derived structure involves using the same tree, but windowing it to limit the number of states is shown as the windowed structure in Fig. 23. For the windowed structure, an additional parameter W may be defined as the size of the window into the tree. In this way, only W states at any trellis stage M are kept where the first state index is defined as B_M (the base state). In order to find B_M at time $M+1$ the window

position may be chosen based on the probability of the states $S_{M, BM}$ through $S_{M, BM + \Delta_{max} - 1}$ compared to $S_{M, BM + W - 1}$ down to $S_{M, BM + W - \Delta_{max}}$.

[00121] The result may be called a ‘folded’ structure (also simply the ‘trellis’ structure). In this structure there are precisely N states at each stage M . In order to accomplish this, the tree structure may be folded such that state $S_{M, t}$ is mapped into state $Z_{M, t \% N}$, where $\%$ denotes the modulo operator into positive integers (i.e. $(-1) \% N = N - 1$). In order to maintain timing in this structure, each state $Z_{M, t}$ has a mapping value t_m that the index of the maximum probability state $S_{M, k}$ that maps into $Z_{M, t}$. At each stage, t_m , to transitions from the state are determined.

[00122] In all of these timing structures, this trellis may be combined with the data trellis and phase trellis to get a combined set of states $S_{M, t, \phi, D}$. Each transition out of this state has a triplet of values $(\Delta_t, \Delta_\phi, b)$ where Δ_t is the timing change and it takes integer values between $-\Delta_{max}$ and Δ_{max} , i.e. $-\Delta_{max}, \Delta_{max} + 1, \dots, -1, 0, 1, \dots, \Delta_{max} - 1, \Delta_{max}$, Δ_ϕ is the phase change, and b is the data bit. In the case of any binary waveforms (e.g. FM0 and Miller), the data metric

for this state and transition is $\text{Re} \left\{ e^{-j(\phi + \Delta_\phi)} \sum_{i=0}^{N-1+\Delta_t} c_{D, b, i} \times r(M \times N + t) \right\}$ where

$c_{D, b, i} = d_{D, b, k} \times (1 - \text{off}) + d_{D, b, k+1} \times \text{off}$ and $d_{D, b, k}$ is an ideal symbol at the nominal sample

rate, where $k = \lfloor i \times \frac{N + \Delta_t}{N} \rfloor$ and $\text{off} = \left(i \times \frac{N + \Delta_t}{N} \right) - k$. Note that for the ‘folded’ version, t_m

is used in place of t .

[00123] In order to capture the timing information with symbol timing that can drift over time, another natural structure of the timing state diagram is a tree structure such as shown in 21-2 where the root node is extended. Assume the nominal timing is N samples per symbol. This means that the granularity of the timing captured from the tree structure will be $\frac{1}{N}$. In order to improve the performance of the trellis, this can be limited to an arbitrary rate R . To do this, the states that would fall outside the bounds of the expected drift are eliminated. If the states are numbered for the first stage of the trellis as S_0 to S_{N-1} for the first stage, the second stage would be numbered $S_{0 - \Delta_{max}}$ to $S_{N + \Delta_{max}}$, and for stage M they would be $S_{0 - M \times \Delta_{max}}$ to $S_{N + M \times \Delta_{max}}$. For this M th stage the states $S_{0 - M \times \Delta_{max}}$ up to but not including $S_{0 - \lceil R \times M \rceil}$

would be elided and also states above $S_{N-1+\lceil R \times M \rceil}$. Each state in this structure has a T_s associated with it that is $M \times N + i$ for state S_i at time M .

[00124] In order to reduce the complexity of the structure, either a ‘folded’ tree or a ‘windowed’ tree can be used. The ‘folded’ tree is a tree where node S_i is mapped to $S_{(i + N) \% N}$ and the T_s associated with the node is the T_s associated with the maximum state value between the mapped states. This means that the transitions become symmetric as in a true trellis, but the transitions carry both a metric and a time with them. In a ‘windowed’ tree structure, an arbitrarily sized window of states is maintained. This window is selected by comparing the probabilities of the edge states. In the case of a windowed tree, one only needs to keep track of T_s for the first state in the window (all other states will be offset linearly from that state). This provides an advantage of smaller storage and simpler implementation.

[00125] Combined Metrics for Data and Timing

$$\sum_{i=1}^{N+\Delta t} d_m(i) \times r(T_s + i)$$

Where

- $r(i)$ is the sample at time i
- $d(i)$ is the ideal symbol sampled at the sample rate (for the data state and input data from the trellis)
- $d_m(i)$ is the interpolated version of ideal symbol.
- T_s is the time stored in the state.

$$p = \lfloor i \times \frac{N + \Delta t}{N} \rfloor$$

- $off = \left(i \times \frac{N + \Delta t}{N} \right) - p$
- $d_m(i) = d(p) \times (1 - off) + d(p + 1) \times off$

An example for is given for the case of $N=4$, $R=10\%$, $M=4$ in 22-2 and 22-4.

[00126] Referring now to Fig. 24, a SISO decoder can be viewed as consisting of four consecutive operations:

- 1) data metric generation and phase rotation
- 2) Branch metric generation and forward node update
- 3) Backward pass node update

4) Extrinsic generation and output

[00127] Basically, the decoder structure can be viewed as a trellis of nodes arranged in columns. Each column corresponds to one symbol of the data stream to be decoded. The nodes within the columns represent the possible combinations of the relevant parameters for the symbol; in particular, the timing, phase, and symbol states. Each contains a numerical value proportional to the computed probability of the parameters which it represents. For FM0, one can use 512 nodes per column corresponding to the combinations of the 16 possible (quantized) phase states, the 16 possible timing states, and the two possible symbol values (0 and 1). The decoder operates by estimating the probability of each node's combination of parameters using metrics derived from the input data. First, probabilities for the nodes within columns are updated in the forward time direction, and then in reverse working backwards through the trellis. When these updates have been completed, the highest computed probability values through the trellis are chosen for the decoded output.

[00128] The inputs to the SISO decoder trellis computation are the data metrics which are derived from the sampled input stream. These are complex numbers, derived from S_i sample values containing both I and Q components. Although there are a total of twelve data metrics which must be computed for each discrete sample time, N , six of these are simply negatives of the others as selected by D , the current data symbol state. The metrics, $M_N(\Delta t, D, d)$, where $\Delta t = \{-1, 0, +1\}$ for timing change, $D = \{0, 1\}$ for current data state, and $d = \{0, 1\}$ for the next symbol value, may be computed from intermediate variables A , B , C , D , E , and F where:

$$\begin{aligned}
 A &= \sum S_i, (n \leq i \leq n+7) &&= \text{sum of 8 samples starting at time } n \\
 B &= \sum S_i, (n+8 \leq i \leq n+15) &&= \text{sum of 8 samples starting at time } n + 8 \\
 C &= \sum S_i, (n \leq i \leq n+6) &&= \text{sum of 7 samples starting at time } n \\
 D &= \sum S_i, (n+8 \leq i \leq n+14) &&= \text{sum of 7 samples starting at time } n + 8 \\
 E &= \sum S_i, (n \leq i \leq n+8) &&= \text{sum of 9 samples starting at time } n \\
 F &= \sum S_i, (n+9 \leq i \leq n+16) &&= \text{sum of 8 samples starting at time } n + 9
 \end{aligned}$$

[00129] Referring now specifically to Fig. 24, the Intermediate Metric Variable Computation is shown. The FM0 data metrics $M_N(\Delta t, D, d)$, can then be derived from the intermediate variables as follows:

$$\begin{aligned}
 M_N(0, 0, 0) &= A_N - B_N &&= -M_N(0, 1, 0) \\
 M_N(1, 0, 0) &= A_N - F_N &&= -M_N(1, 1, 0) \\
 M_N(-1, 0, 0) &= C_N - D_N &&= -M_N(-1, 1, 0) \\
 M_N(0, 0, 1) &= A_N + B_N &&= -M_N(0, 1, 1)
 \end{aligned}$$

$$\begin{aligned} M_N(1,0,1) &= E_N + F_N &= &-M_N(1,1,1) \\ M_N(-1,0,1) &= A_N + D_N &= &-M_N(-1,1,1) \end{aligned}$$

[00130] Regarding phase rotation, the node update operation does not use the M_N directly, but rather uses the real portion of the complex data metric vector as rotated by the interpolated phase, ϕ , for each trellis branch. The rotated data metric is expressed as $R_N(\phi) = \text{Re}[M_N * e^{j\phi}]$. Since there are only sixteen evenly spaced discrete values for the node phase state, the interpolated branch phase can only take on 32 values and the product computation is greatly simplified. This is shown in the table below. Due to symmetry, 16 of the values are simply derived by negation of those calculated π radians away. This means that all 32 rotations can be computed using 14 multipliers and 14 adder/subtractors. By sequencing the 6 values for M_N as input into the phase rotator block, all 32 rotations of all twelve metrics may be computed in real-time at the sample rate. The outputs are fed to the node processors for branch metric computation where they are added or subtracted as needed.

[00131] Regarding backwards pass data metric storage and sequencing, the rotated data metrics must also be fed to the node update mechanism for the backwards node update pass. This requires either storage of the values computed for the forward pass, or else regeneration from either the data or data metrics. In either case storage memory is necessary. Using a 256-bit packet for purposes of illustration, storage of the rotated data metrics would require: $16 \times 6 \times 16 \times 256 = 393,216$ (16-bit) words of storage. At the other extreme, storage of the interpolated input data stream would require only $2 \times 16 \times 256 = 8192$ words of storage. While storing the interpolated data alone would save substantial memory, it requires that the metric generation shift-register (as shown above) be run in the reverse direction (from right-to-left), with the stored data fed to it reversed in time, in order to derive the data metrics for the backwards pass. The data resurrected data metric values must be fed to the phase rotator as before. The $R_N(\phi)$ outputs must, however, be resequenced for presentation to the node processors. Recall that for the data metrics, $M_N(\Delta t, D, d) = -M_N(\Delta t, \sim D, d)$. This allowed the nodes with $D=1$ during the forward update pass simply to be fed the negatives of the $R_N(\phi)$'s for their $D=0$ counterparts. During the backwards pass, however, we are indexing the node processors by d instead of D since our source nodes are now later in time. Consequently, the $M_N(\Delta t, D, d)$ are no longer the arithmetic complements for $d=0$ vs. $d=1$; and instead the proper $R_N(\phi)$ must be stored, sequenced, and fed to the node processors.

[00132] Regarding branch metric generation and node updating, the branch metrics, B_{XY} , where X is the originating node within symbol column C, and Y the destination node in column C+1, are calculated as

$$B_{XY} = d * S_C + R_N(\varphi, \Delta t, D, d) + U(\Delta \varphi) + V(\Delta t)$$

Where d = the destination data state (i.e. input data bit value)

S_C = Soft input value for column C

$R_N(\varphi, \Delta t, D, d) = \text{Re}[M_N(\Delta t, D, d) * e^{j\varphi}]$, the rotated data metric

$U(\Delta \varphi)$ = one value for $\Delta \varphi = 0$, another for $\Delta \varphi = +1, -1$

$V(\Delta t)$ = one value for $\Delta t = 0$, another for $\Delta t = +1, -1$

[00133] For FM0, there are 18 branches out of each source node, corresponding to the 3 values for $\Delta \varphi$, times the 3 values for Δt , times 2 values for d . Accordingly there are also 18 branches into each destination node. To update the probability score, Q_Y , for a destination node, the Q_X from the source node is added to the branch metric for all input branches leading directly to node Y. The value for the branch with the greatest sum is then selected and stored for Q_Y . The associated sample time value, T_Y , must also be stored, where $T_Y = T_X + 16 + \Delta t$ (or for reverse updates: $T_Y = T_X - 16 - \Delta t$), and T_X is the stored time value from the source node for the selected branch.

Table for Phase RotationData Metric $M_N = x + jy$

$$\begin{aligned}
 a &= \cos(\pi/8), & b &= \sin(\pi/8) \\
 c &= \sin(\pi/4) = & \cos(\pi/4) \\
 d &= \cos(\pi/16), & e &= \sin(\pi/16) \\
 f &= \cos(3\pi/16), & g &= \sin(3\pi/16)
 \end{aligned}$$

Angle φ	$e^{j\varphi}$ Real Part	$e^{j\varphi}$ Imaginary Part	Real Part of Metric Product
0	1	0	x
$\pi/16$	d	e	dx - by
$\pi/8$	a	b	ax - by
$3\pi/16$	f	g	fx - gy
$\pi/4$	c	c	cx - cy
$5\pi/16$	g	f	gx - fy
$3\pi/8$	b	a	bx - ay
$7\pi/16$	e	d	ex - dy
$\pi/2$	0	1	-y
$9\pi/16$	-e	d	-ex - dy
$5\pi/8$	-b	a	-bx - ay
$11\pi/16$	-g	f	-gx - fy
$3\pi/4$	-c	c	-cx - cy
$13\pi/16$	-f	g	-fx - gy
$7\pi/8$	-a	b	-ax - by
$15\pi/16$	-d	e	-dx - gy
π	-1	0	-x
$17\pi/16$	-d	-e	-dx + ey
$9\pi/8$	-a	-b	-ax + by
$19\pi/16$	-f	-g	-fx + gy
$5\pi/4$	-c	-c	-cx + cy
$21\pi/16$	-g	-f	-gx + fy
$11\pi/8$	-b	-a	-bx + ay
$23\pi/16$	-e	-d	-ex + dy
$3\pi/2$	0	-1	y
$25\pi/16$	e	-d	ex + dy
$13\pi/8$	b	-a	bx + ay
$27\pi/16$	g	-f	gx + fy
$7\pi/4$	c	-c	cx + cy
$29\pi/16$	f	-g	fx + gy
$15\pi/8$	a	-b	ax + by
$31\pi/16$	d	-e	dx + ey

[00134] Regarding the data-driven update mechanism, the 16 values output from phase rotation for the rotated data metrics, $R_N = \text{Re}[M_N * e^{j\varphi}]$ for $D = 0$; $\varphi = 0, \pi/8, \pi/4, 3\pi/8, 3\pi/2, 13\pi/8, 7\pi/4$, and $15\pi/8$, and specified N , d , and Δt ; are fed to the node update mechanism. Since the remaining phase angles can also be derived from these 16 simply by negating the corresponding value π radians away; and since the values of the R_N for $D=1$ are also just the negatives of those for $D=0$; each set of the eight R_N values is sufficient for metric generation for the three branches ($\Delta\varphi = -1, 0, +1$) from up to 32 source nodes (all nodes of the specified time state N) in the originating symbol column, C . These R_N values may be labeled as negated for specified values of φ and D as $R_{N\varphi D}$. For forward update, the $R_{N\varphi D}$ are fed into 32 node processors. These processors compute the branch metrics B_{XY} and sum them with the stored source node values, Q_X . The branch sums are passed to 16 branch selection units which compare six input branch values and select the largest for output. Each selection unit corresponds to a specific phase value, φ_Y . The inputs are then the branches where $\varphi_Y = \varphi_X - (\Delta\varphi * \pi/8)$, including the branches for both $d=0$ and $d=1$. The outputs of these selection units then feed back to the two node processors of corresponding phase where they are used to update the stored Q_Y value for the destination node. A minimum of ninety-six clocks are required to update each symbol column. For the reverse update direction, the rotated metrics are regenerated starting with the most recent symbol, and proceeding back to the first. The later column nodes (to the right in the trellis) are used for the source values, Q_X , and the earlier column to the left are now updated as the Q_Y .

[00135] Referring now to Fig. 25, the interconnection of node processors and branch select units are shown. For convenience, upwards arrows to $\Delta\varphi = +1$ for forward updates, -1 for backwards updates. Downwards arrows are for branches with $\Delta\varphi = -1/+1$ for forward/backward updates. Horizontal arrows are for $\Delta\varphi = 0$.

[00136] Referring now to a source node processor, the proposed implementation consists of 32 node processors, each assigned to a particular data state value (0 or 1), and phase state (0 to 15). One of the eight R_N values, or its arithmetic complement, as appropriate, are fed into each node processor corresponding to its assigned data and phase state values. Each processor consists of a node memory, a comparator, and four adders. This structure is shown in the diagram below. The node memory stores two values for each node, the probability score Q ,

and the time code T . Each processor's node memory contains all trellis nodes for a specific data state, D , and for a specific phase state value, ϕ . It also contains the storage for the nodes in all trellis symbol columns, C , and for all sixteen time state values, N . For a 256 symbol decoder, $16 \times 256 = 4096$ node storage locations would be required. Local storage can be greatly reduced for large message sizes if paging to external memory is implemented.

[00137] The adders function to generate three branch metrics on each clock as the six R_N 's are fed in sequentially for each N . Therefore, a minimum of 96 clock cycles are required to update a symbol column. The adders serve to sum the various terms for the branch metric values B_{XY} with the source node value, Q_X . The value $d \cdot S_C$, being global to all processors, is developed externally. The value for $V(\Delta t)$ is also selected outside and summed with $d \cdot S_C$ to be fed to the node processors as an input. Remaining inputs are the symbol column number C , which is concatenated with the timing sample state N to address a particular node within local storage; the rotated metric value $R_{N\phi D}$, and the two values for $U(\Delta\phi)$.

[00138] Referring now to destination node processing, as the $R_{N\phi D}(d, \Delta t)$ are fed into the source node processors, sequentially stepping through the six combinations of d and Δt for each sample time N , the $B_{XY} + Q_X$ sums are output to the destination nodes for comparison and selection. Since d is fixed at each clock, there are only sixteen destination nodes for the 96 branches generated on each clock. This means there are six potential branches into each destination node at each clock which need to be compared and selected for the maximum. Along with the branch sum, the corresponding time value, T_X , from the source node for the winning branch must also be selected and stored. Destination processing can be performed by a seven-input maximum selector. The seventh input is used to compare any previous maximum partial results from the three update cycles required to examine all eighteen of the branches into a destination node. The results of each of these sixteen selectors is shared as input to the two node memories sharing the same time state value, N , but one with $D=0$, and one with $D=1$. It should be noted that the destination node N_Y time-state value is not necessarily the same as the source N_X value, but is rather equal to $(N_X + \Delta t)$ modulo 16.

[00139] Referring now to time divergence, a possible problem with the basic source node processing as shown in the diagram above lies in the way in which the trellis tracks timing. There are several timing variables of interest. T refers to absolute sample time as numbered sequentially from the first data sample. Each node in the trellis also has a fixed 4-bit timing

state value, N , ranging from 0 to 15. This 4-bit value always corresponds to the LS 4-bits of the absolute sample time assigned to that particular node. That assigned T can, however, change within the symbol column depending upon T_{XY} value for the branch selected during node update, where $T_{XY} = T_X + \Delta t$. This T_{XY} value should therefore be stored in the node when it is updated. When generating the branch metric values, it may be necessary to compare the stored T_X for the node with the sample time $T_{N\phi D}$, as it is possible for the stored T assigned to a node with timing state N , to be different. This means that with the basic architecture of the diagram, multiple passes may be needed to present the rotated data metric for all node T values at a given N , ϕ , and D in order to generate all of the branch metrics. This is the reason for the equality comparator and the valid line shown in the diagram. In order to increase parallelism and reduce the number of clock passes required, it is highly desirable to present several possible rotated metrics in parallel to the node processor so that branches for varying T 's, but with specified N , can be generated simultaneously. Source node processing architecture for multiple parallel T updates is shown below. Since total divergence is limited by the length of the data packet, and since the LS-4 bits are redundant, it is not necessary that all bits of T_{XY} be stored and compared in the node processor. The additional $R_{N\phi D}$ can be made available by saving the 8 rotated metric values generated for each clock in delay storage of length 96 clocks for each additional $R_{N\phi D}(T)$ to be presented. This requires four 18K block RAM for every two additional values of T , if the RAM is operated at the same clock rate as the branch metric generator.

[00140] Referring now to Fig. 26, the extended parallel source node processing is shown.

[00141] Referring now to Fig. 27, the forward and backward processing is shown.

ϕ	Data Stat e	Phase State	Forward $R_{Nd}(\phi)$	Backward $R_{Nd}(\phi)$
0	0	0	$R_{NX}(0)$	$R_{N0}(0)$
0	1	0	$-R_{NX}(0)$	$R_{N1}(0)$
$\pi/8$	0	1	$R_{NX}(\pi/8)$	$R_{N0}(\pi/8)$
$\pi/8$	1	1	$-R_{NX}(\pi/8)$	$R_{N1}(\pi/8)$
$\pi/4$	0	2	$R_{NX}(\pi/4)$	$R_{N0}(\pi/4)$
$\pi/4$	1	2	$-R_{NX}(\pi/4)$	$R_{N1}(\pi/4)$
$3\pi/8$	0	3	$R_{NX}(3\pi/8)$	$R_{N0}(3\pi/8)$
$3\pi/8$	1	3	$-R_{NX}(3\pi/8)$	$R_{N1}(3\pi/8)$

$\pi/2$	0	4	$-R_{NX}(3\pi/2)$	$-R_{N0}(3\pi/2)$
$\pi/2$	1	4	$R_{NX}(3\pi/2)$	$-R_{N1}(3\pi/2)$
$5\pi/8$	0	5	$-R_{NX}(13\pi/8)$	$-R_{N0}(13\pi/8)$
$5\pi/8$	1	5	$R_{NX}(13\pi/8)$	$-R_{N1}(13\pi/8)$
$3\pi/4$	0	6	$-R_{NX}(7\pi/4)$	$-R_{N0}(7\pi/4)$
$3\pi/4$	1	6	$R_{NX}(7\pi/4)$	$-R_{N1}(7\pi/4)$
$7\pi/8$	0	7	$-R_{NX}(15\pi/8)$	$-R_{N0}(15\pi/8)$
$7\pi/8$	1	7	$R_{NX}(15\pi/8)$	$-R_{N1}(15\pi/8)$
π	0	8	$-R_{NX}(0)$	$-R_{N0}(0)$
π	1	8	$R_{NX}(0)$	$-R_{N1}(0)$
$9\pi/8$	0	9	$-R_{NX}(\pi/8)$	$-R_{N0}(\pi/8)$
$9\pi/8$	1	9	$R_{NX}(\pi/8)$	$-R_{N1}(\pi/8)$
$5\pi/4$	0	10	$-R_{NX}(\pi/4)$	$-R_{N0}(\pi/4)$
$5\pi/4$	1	10	$R_{NX}(\pi/4)$	$-R_{N1}(\pi/4)$
$11\pi/8$	0	11	$-R_{NX}(3\pi/8)$	$-R_{N0}(3\pi/8)$
$11\pi/8$	1	11	$R_{NX}(3\pi/8)$	$-R_{N1}(3\pi/8)$
$3\pi/2$	0	12	$R_{NX}(3\pi/2)$	$R_{N0}(3\pi/2)$
$3\pi/2$	1	12	$-R_{NX}(3\pi/2)$	$R_{N1}(3\pi/2)$
$13\pi/8$	0	13	$R_{NX}(13\pi/8)$	$R_{N0}(13\pi/8)$
$13\pi/8$	1	13	$-R_{NX}(13\pi/8)$	$R_{N1}(13\pi/8)$
$7\pi/4$	0	14	$R_{NX}(7\pi/4)$	$R_{N0}(7\pi/4)$
$7\pi/4$	1	14	$-R_{NX}(7\pi/4)$	$R_{N1}(7\pi/4)$
$15\pi/8$	0	15	$R_{NX}(15\pi/8)$	$R_{N0}(15\pi/8)$
$15\pi/8$	1	15	$-R_{NX}(15\pi/8)$	$R_{N1}(15\pi/8)$

[00142] Extrinsic generation may be performed as the nodes are updated in the reverse direction. A reliability measure is also computed. The extrinsic is computed as $\text{Max}(\alpha_X + B_{XY} + \beta_Y)$ over each column.

[00143] It is clear to a person having ordinary skill in this art that the techniques described above may be applied to a communication method or system for processing modulated signal with random data, and/or phase and/or unknown timing to estimate received data sequences or packetized data. The receiver may use iterative processing with soft-input-soft-output (SISO) components to combine channel decoding with equalization, demodulation, phase tracking, symbol timing, synchronization and interference cancellation as part or in whole. These techniques may be used for any wireless communication systems to model the observation space. These techniques may be used for sensory receiver system for detecting signals in presence of noise and channel distortion utilizing iterative method to detect the signal. A communication system may use these techniques for maximum likelihood sequence

estimation which may include lattice, trellis or tree structures or products thereof for joint estimation of phase, timing, data and/or baud rate. Such techniques may also be used in signal detection systems utilizing iterative methods for optimal detection of the signal in the presence of white noise and channel distortion such as those employing in-door wireless channels, out-door wireless channels, both line-of-sight or non-line of sight communications, wire line channel such as copper and fiber wires, underground or underwater sonar, recording channels such as hard disk storage and both volatile and non-volatile memory and/or combinations of any of these channels.

[00144] The disclosed techniques are useful in the detection of packetized data with unknown data pulse duration, random phase and unknown data, any combination or thereof. They are useful in digital packet radio systems employing soft-input-soft-output (SISO) decoding methods with or without cascaded iterative decoder and with or without channel encoding/decoding. These techniques may be used in communication systems employing channel coding methods including algebraic block codes, convolution and turbo codes, low density parity check, repeat-accumulate codes, and product codes cascaded with SISO decoders exchanging extrinsic information to optimally decode the user data. Similarly, these techniques may be used in communication systems employing channel coding including coding which can be represented via planar graph such as bipartite, tree or trellis diagram whereby the posteriori probabilities (extrinsic information) of each state can be computed and iteratively improved. Such communication systems may employing belief propagation method to decode the received sequence and exchange extrinsic information with the soft-input-soft-output decoder. A communication system or packet radio timing synchronization may be provided for any modulation scheme such as multi-level phase, position, amplitude in quadrature and in-phase (one or both). Further, such systems may be embedded in portable or stationary devices, in hubs, central office or network edge devices and may be implemented in software, such as a "Software Defined Radio", on special purpose or general purpose host computer and offered as a web service or general purpose signal processing platform.

Claims

1. A method for operating an RFID receiver, comprising:
 - sampling a received signal including RFID data signals from at least one interrogated RFID tag;
 - providing a set of predetermined probabilities of a received signal sample making a specific transition between data states, each predetermined probability related to data, timing and baud rate variables affecting the received signal;
 - applying the set of predetermined probabilities to each of a plurality of pairs of signal samples to determine probabilities of the received signal having made the specific transitions between each of the signal samples in that pair; and
 - processing the determined probabilities to recover RFID data signals by determining a sequence of transitions in the received signal having the highest probability of occurrence.
2. The method of claim 1 wherein each of the predetermined probabilities is also related to a phase variable affecting the received signal.
3. The method of claim 2 wherein the applying the set of predetermined probabilities, and the processing the determined probabilities, are iterated to recover the RFID data signals.
4. The method of claim 3 wherein the set of predetermined probabilities are related to transitions in a first direction, the method further comprising:
 - providing a second set of predetermined probabilities related to transitions in an opposite direction; and
 - applying the second set of predetermined probabilities to each of the plurality of pairs of signal samples to determine second probabilities of the received signal making the specific transitions between each of the signal samples in that pair in the opposite direction; and
 - processing the first and second determined probabilities to recover the RFID signals.

5. The method of claim 4 wherein applying the first and second set of predetermined probabilities, and the processing the first and second determined probabilities, are iterated to recover the RFID data signals.
6. The method of claim 5 wherein the applying and processing are iterated until further iterations do not further change the determined probabilities.

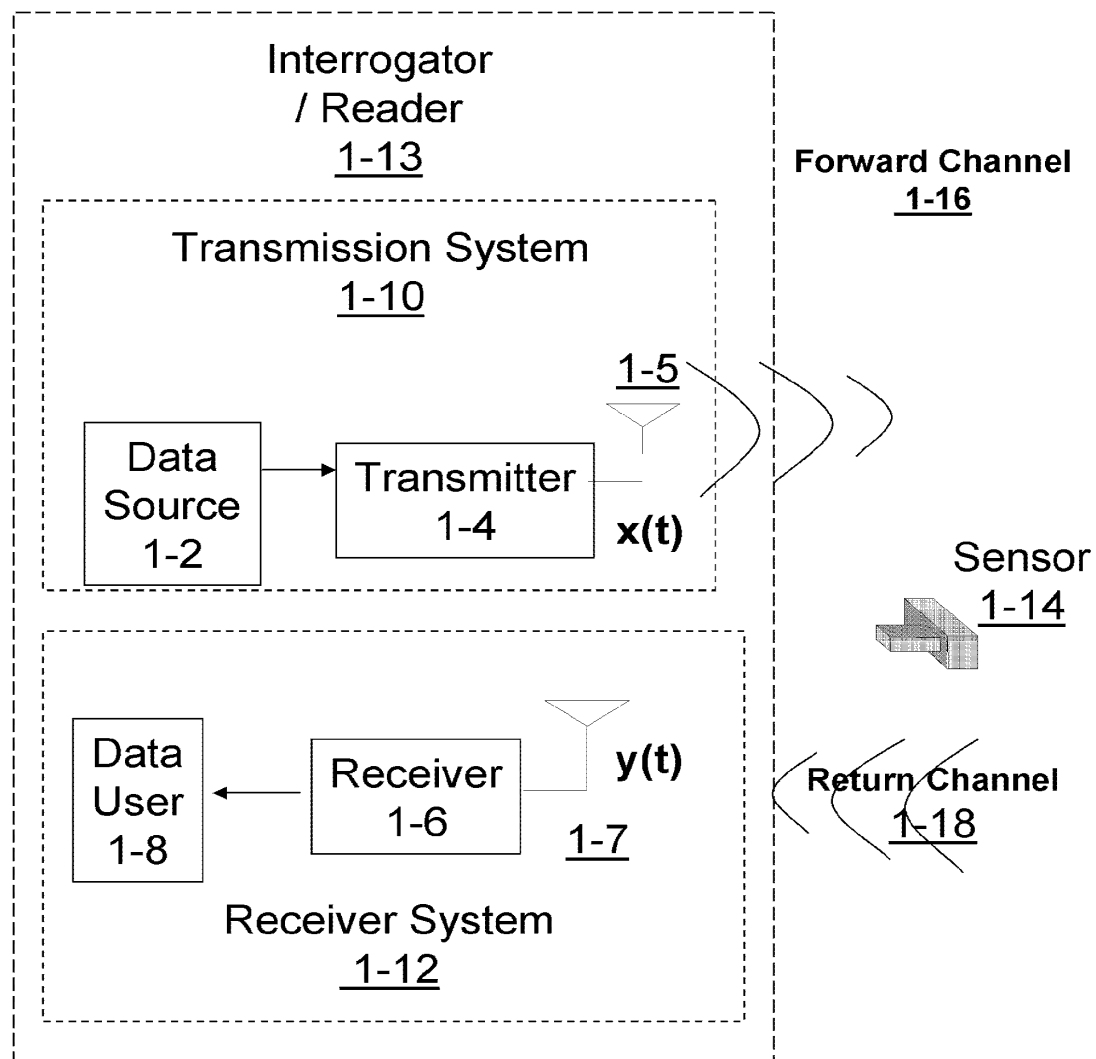


Fig. 1

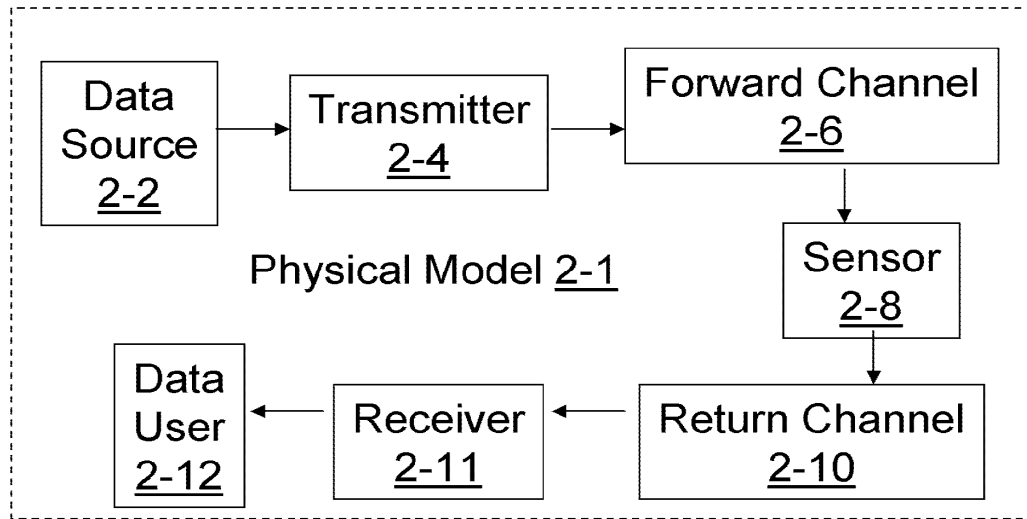


Fig. 2a

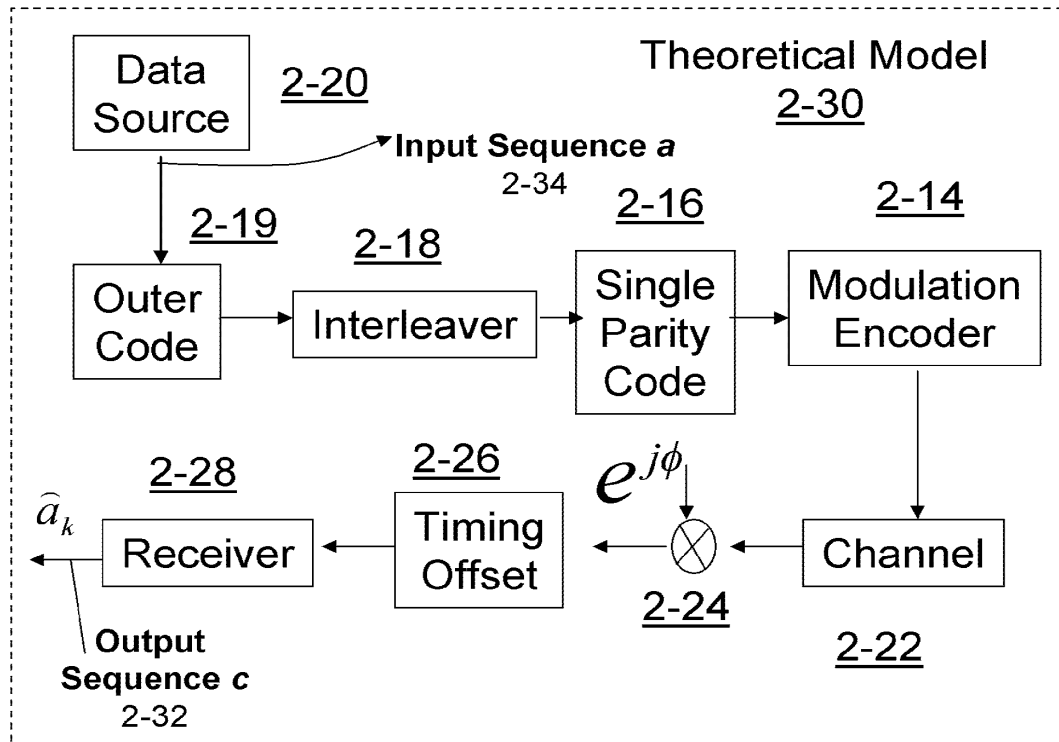


Fig. 2b

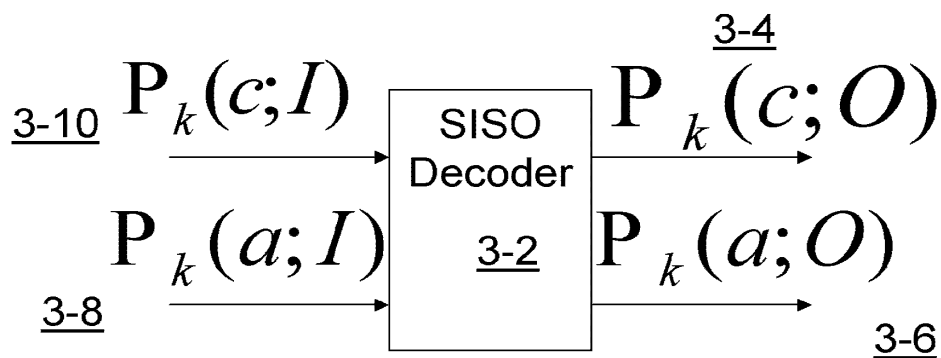


Figure 3.

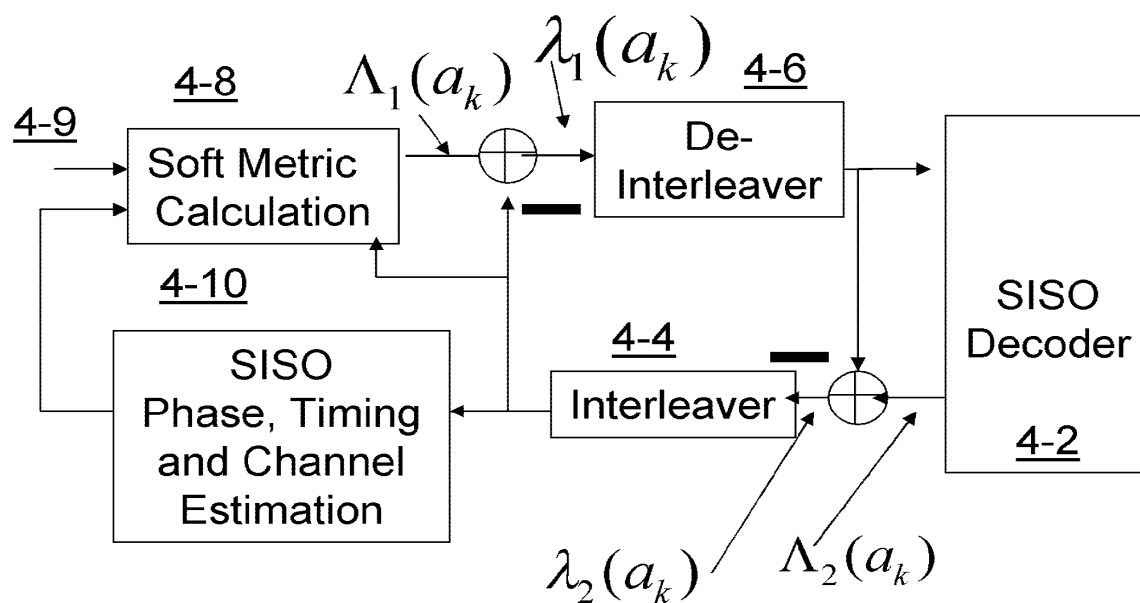


Fig.4

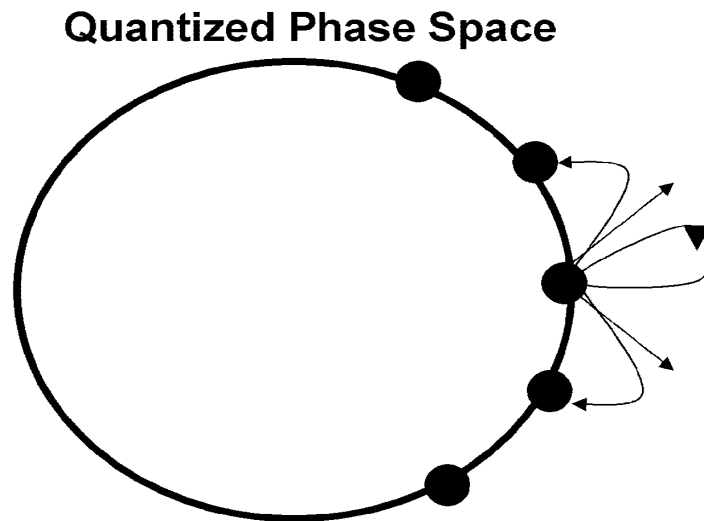


Figure 5.

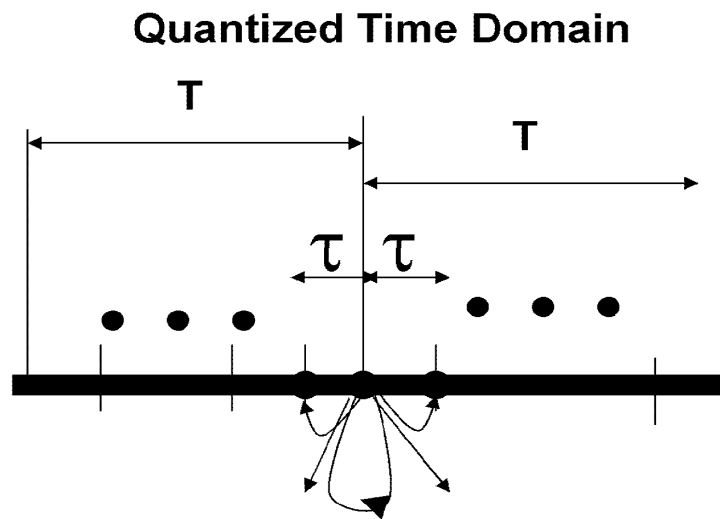


Figure 6.

Example of Trellis Diagram

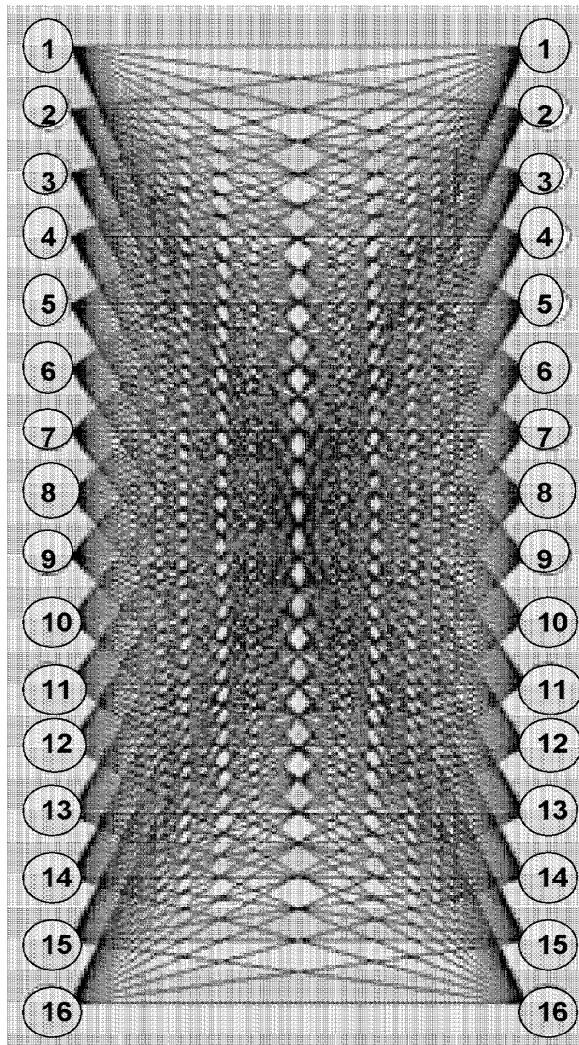
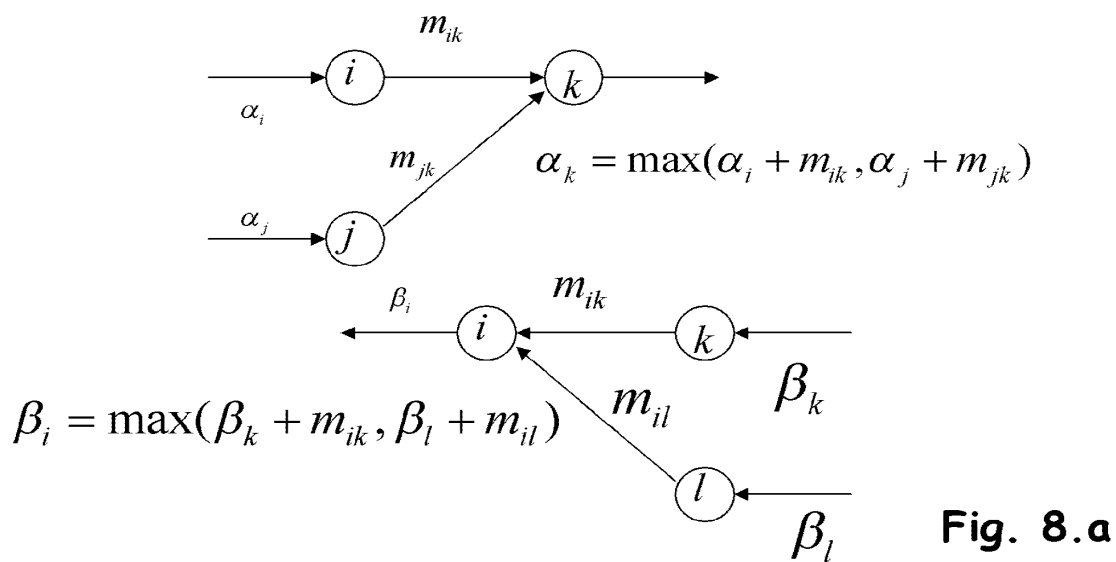
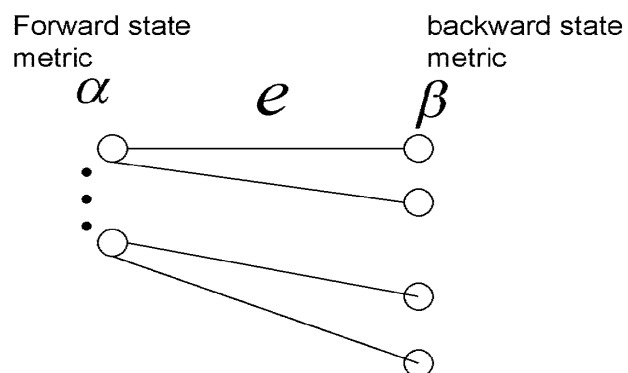


Figure 7.



RFID Channel Code

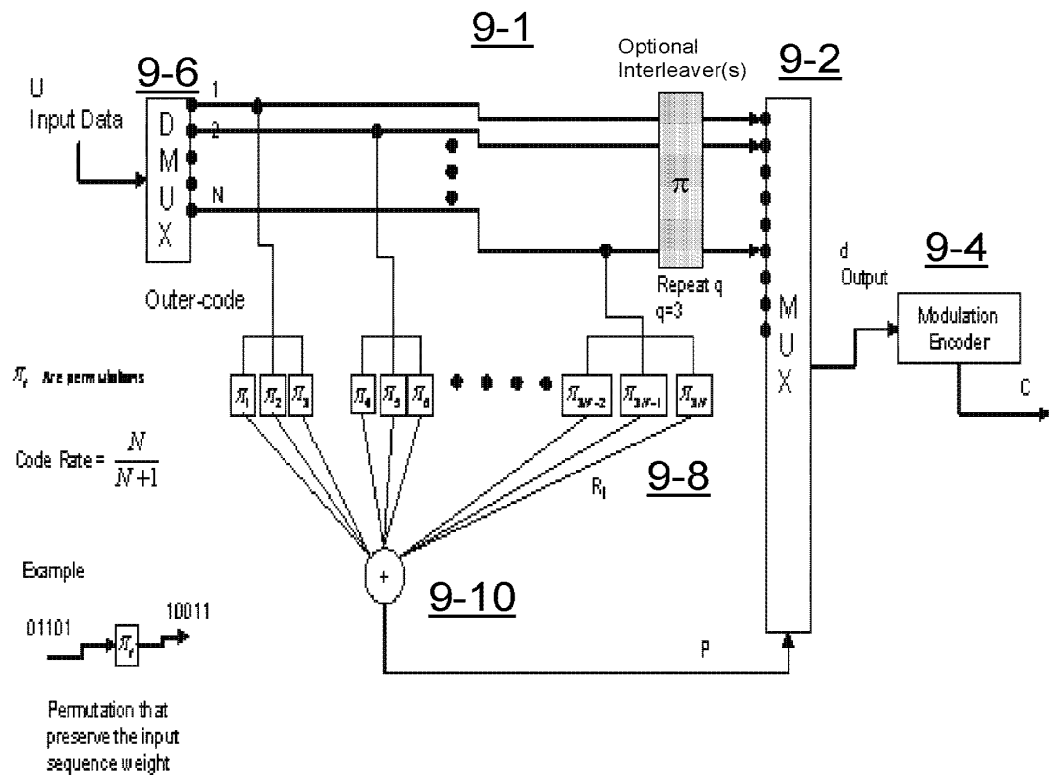


Fig. 9.

Repetition L SISO Decoder

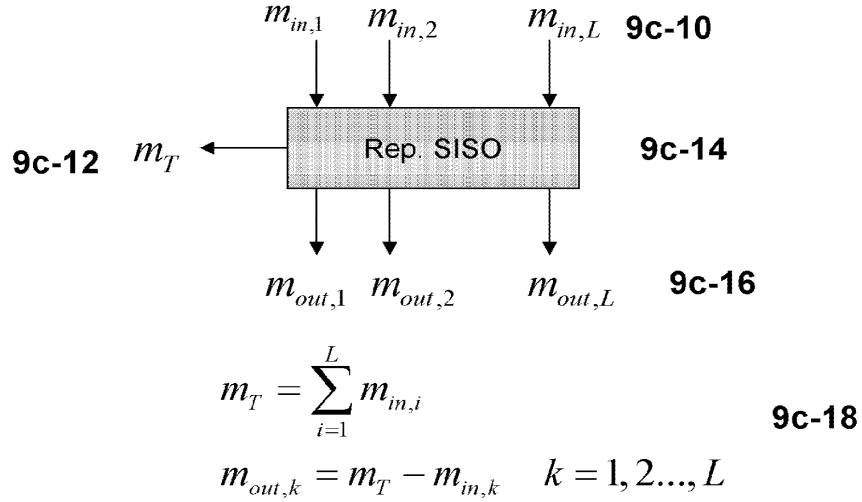


Figure 9c

SPC SISO Decoder With q input one output

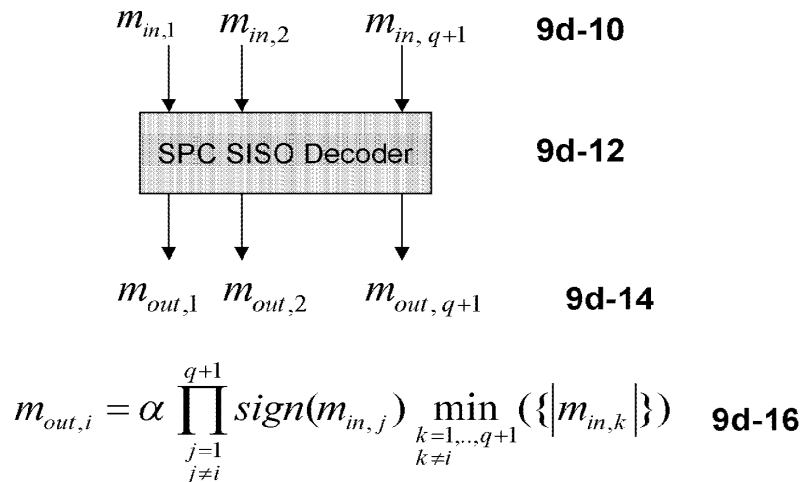


Figure 9d

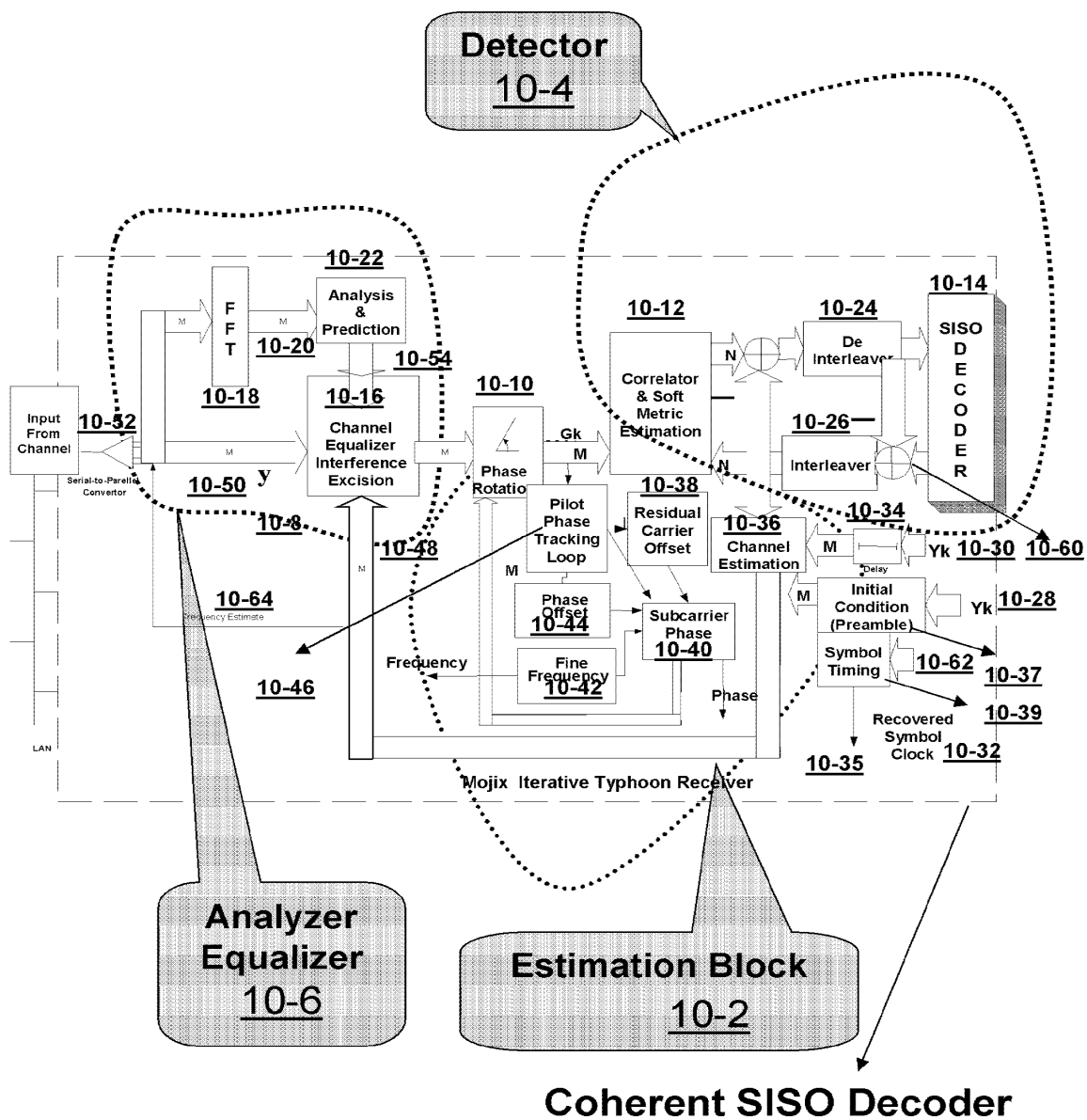


Fig.10

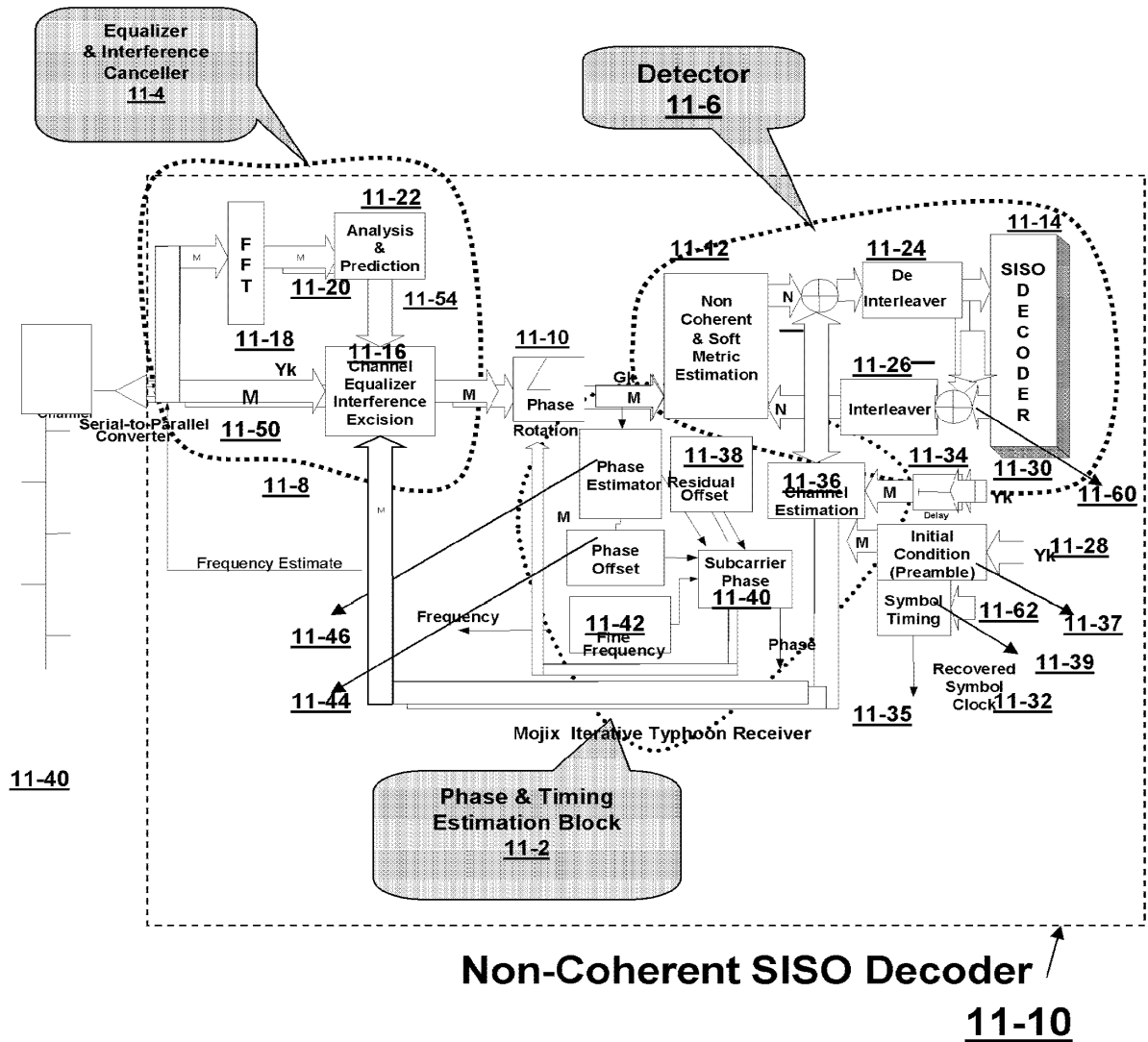


Fig. 11

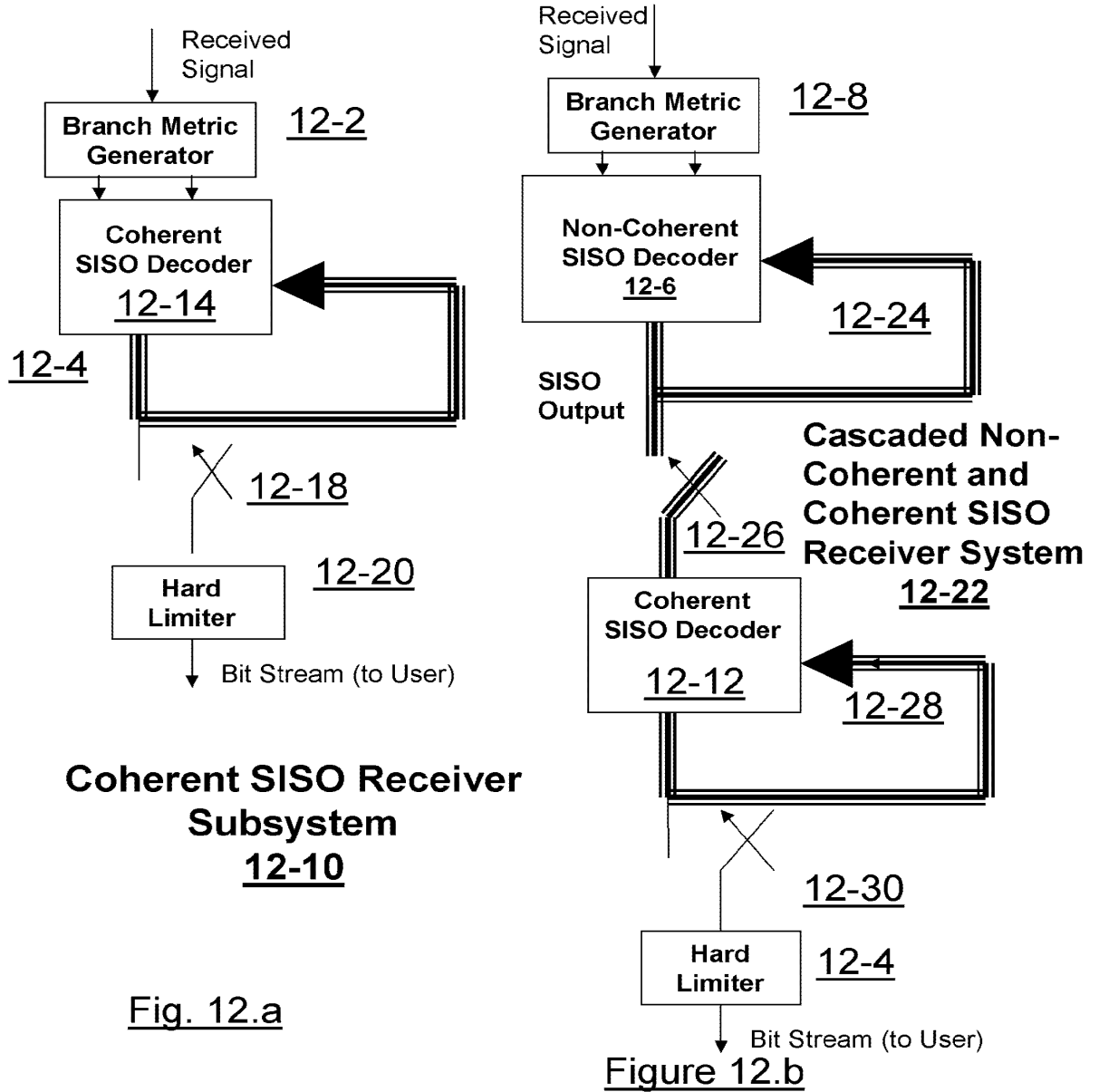


Figure 12.

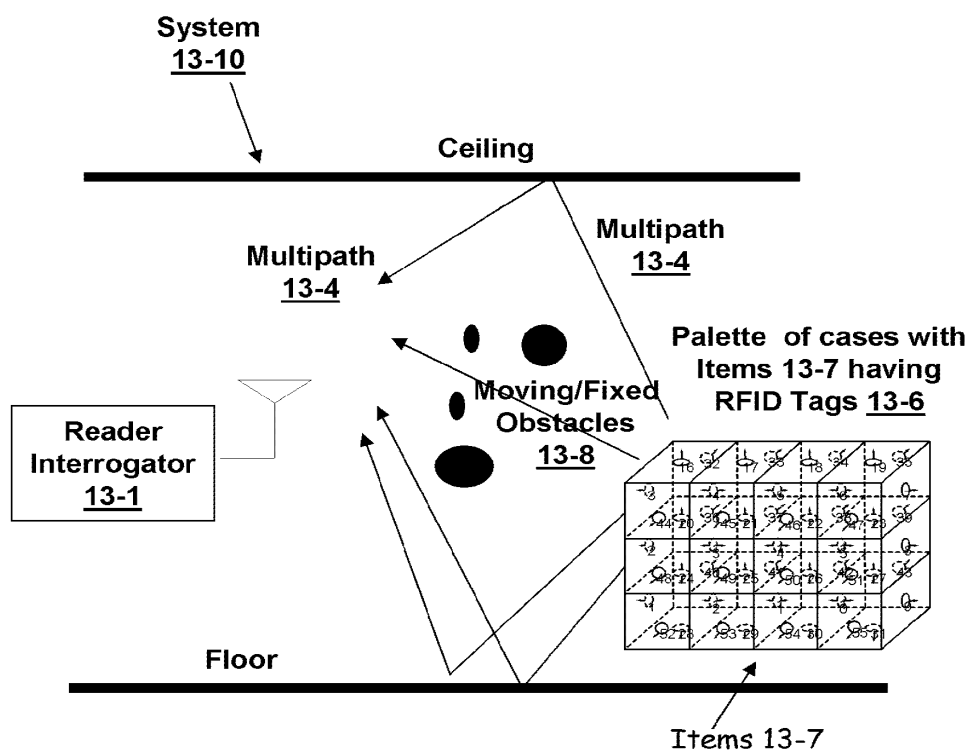
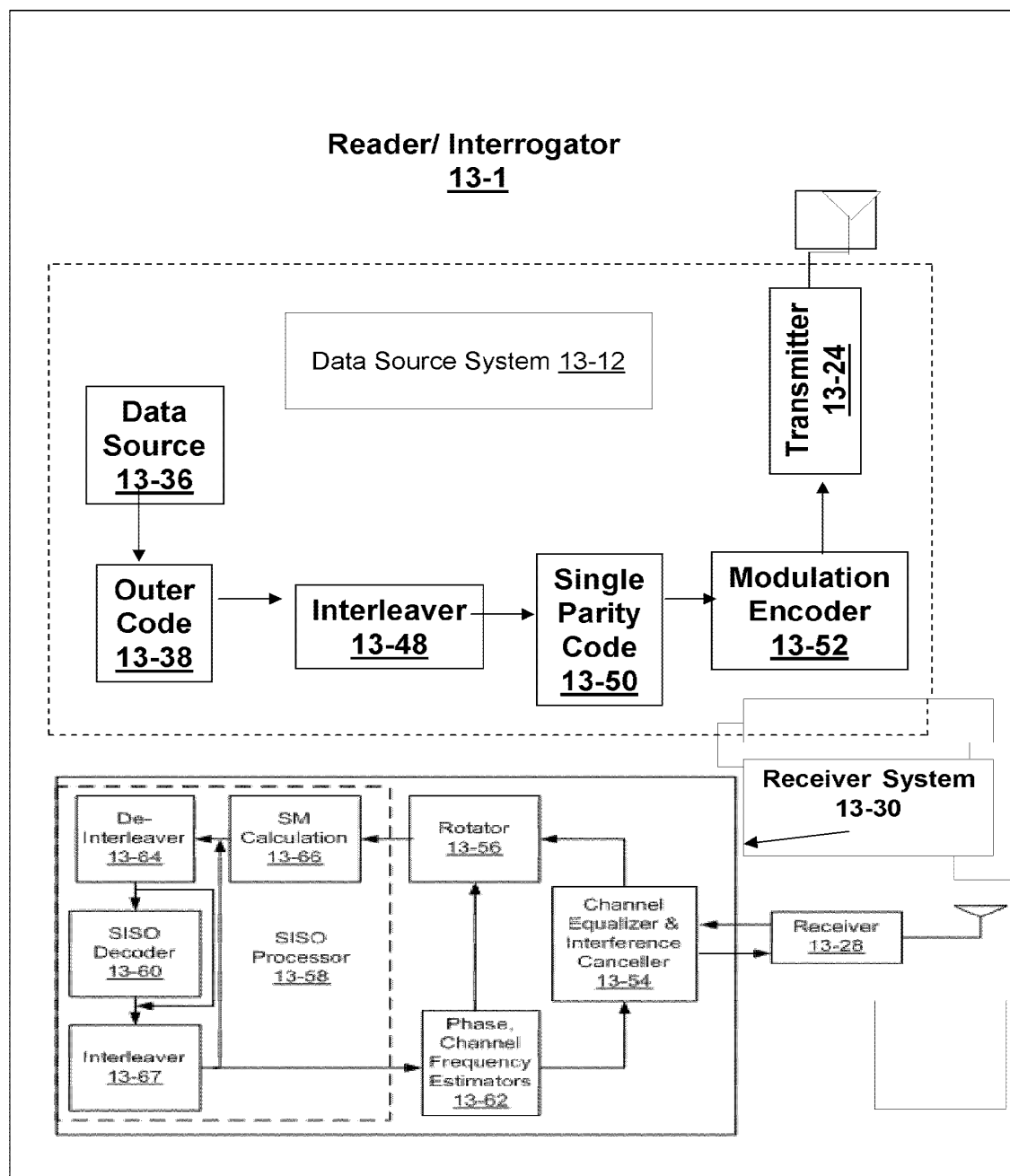


Fig. 13a

**Fig. 13b**

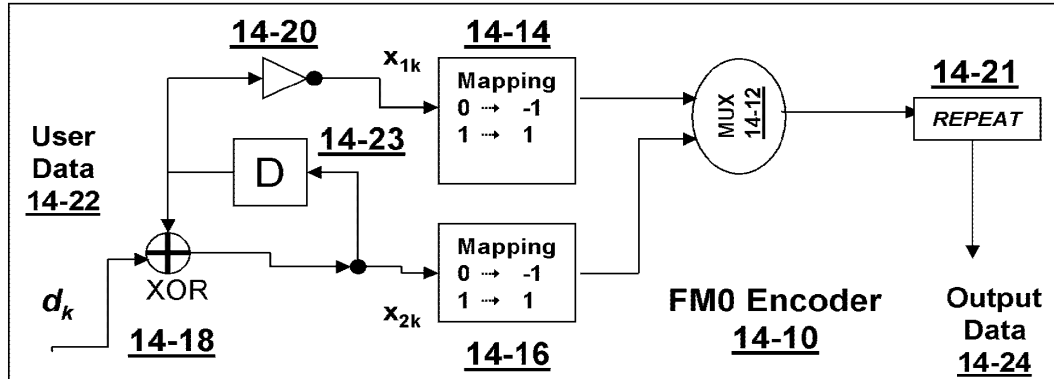


Fig. 14a

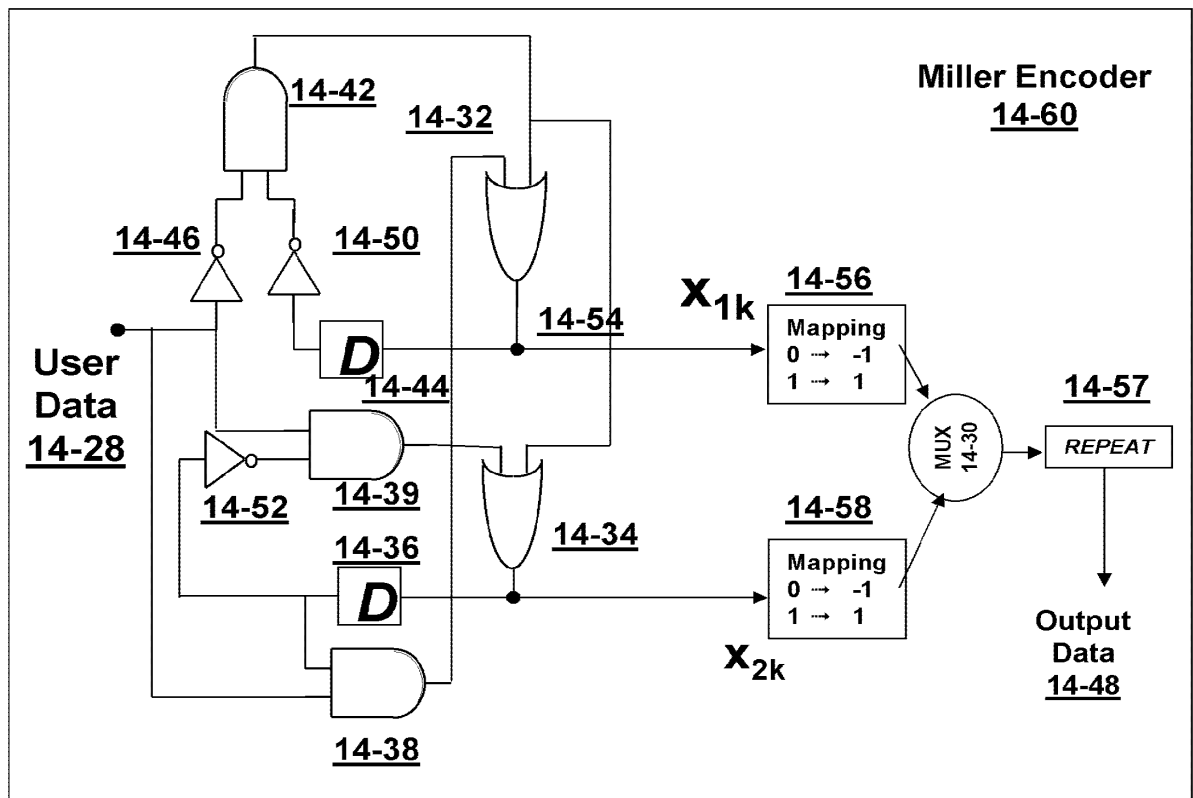
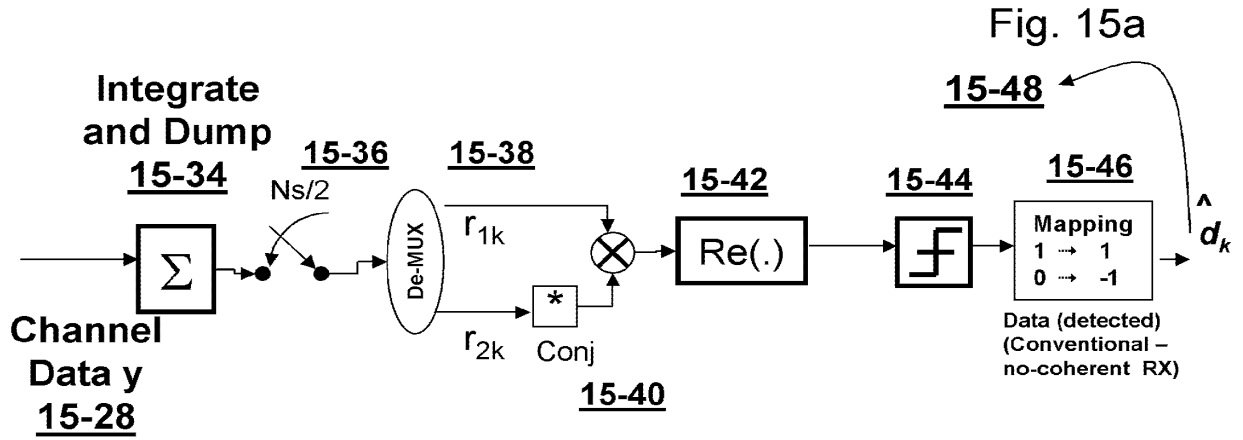
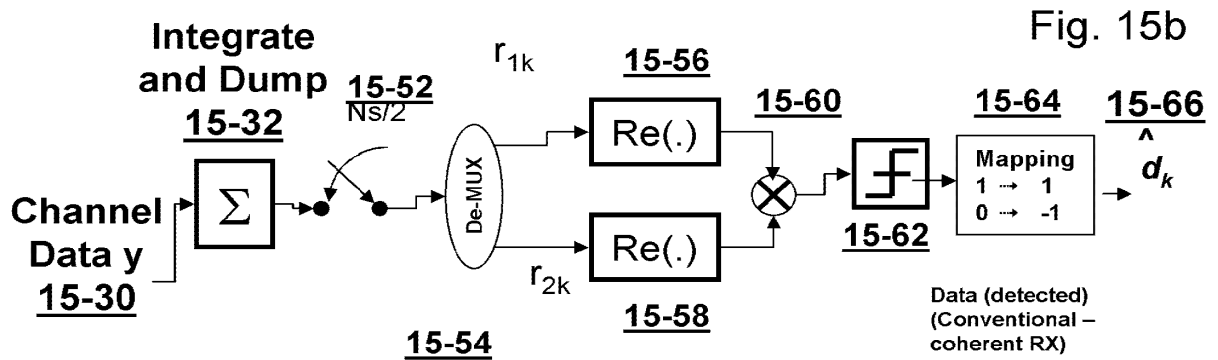
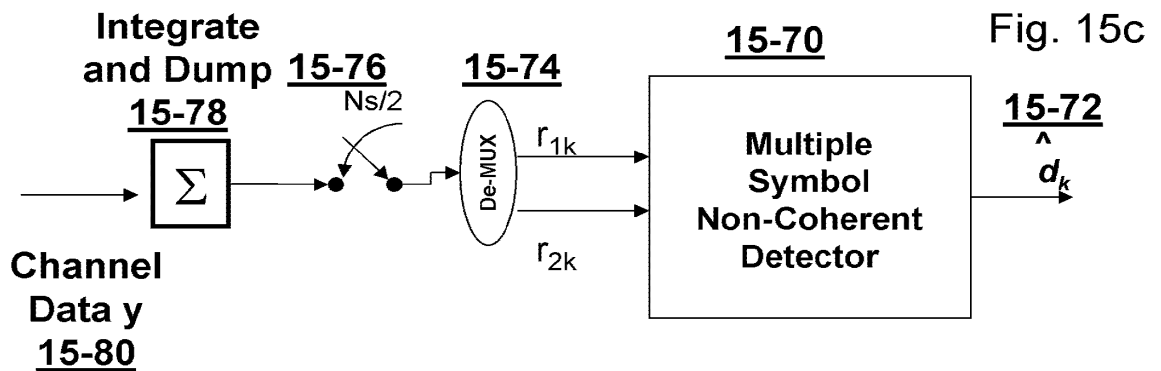
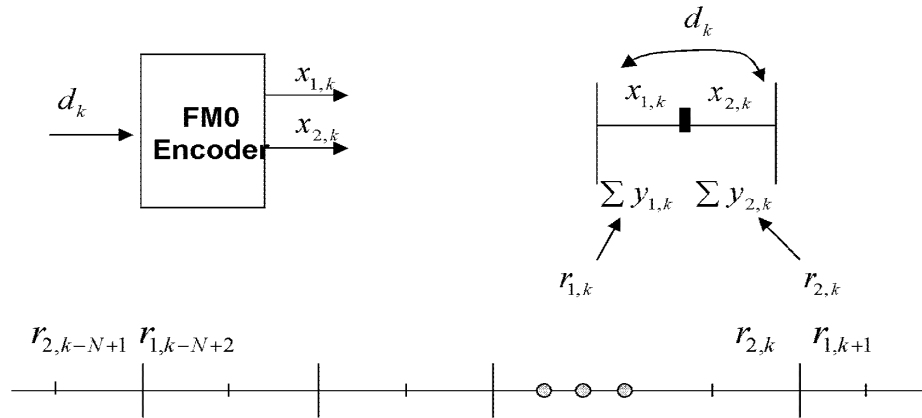


Fig 14.b



FM0 Multi-Symbol Non-Coherent Detection

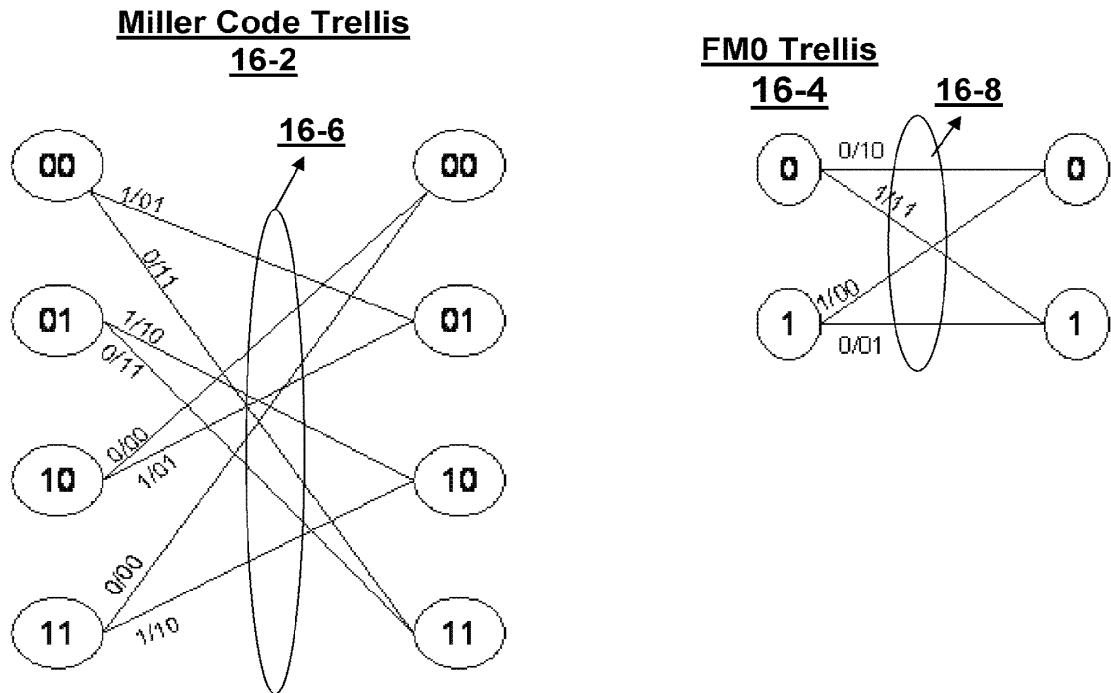
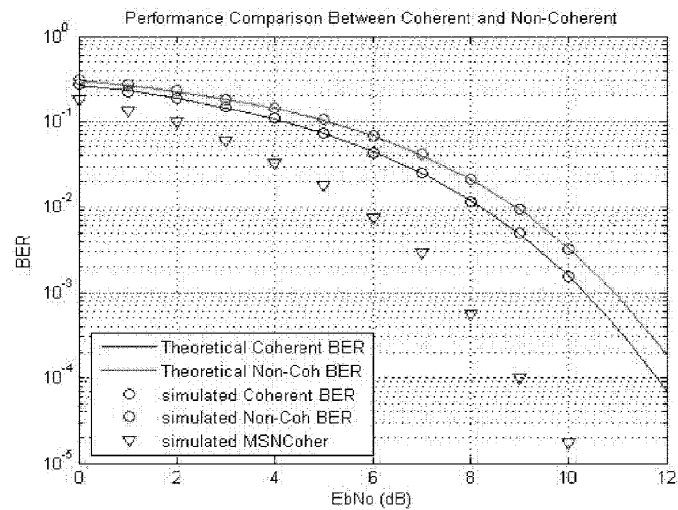


$$(\hat{d}_k, \hat{d}_{k-1}, \dots, \hat{d}_{k-N}) = \arg \max_{d_k, d_{k-1}, \dots, d_{k-N+2}} \left| (r_{2,k-N+1} - r_{1,k-N+2}) + \sum_{i=k-N+3}^{k+1} (r_{2,i-1} - r_{1,i}) \prod_{j=k-N+2}^{i-1} d_j \right|$$

For N=3:

$$(\hat{d}_{k-1}, \hat{d}_k) = \arg \max_{d_{k-1}, d_k} \left| (r_{2,k-2} - r_{1,k-1})d_{k-1} + (r_{2,k-1} - r_{1,k}) + (r_{2,k} - r_{1,k+1})d_k \right|$$

Figure 15d

**Figure 16****Figure 17**

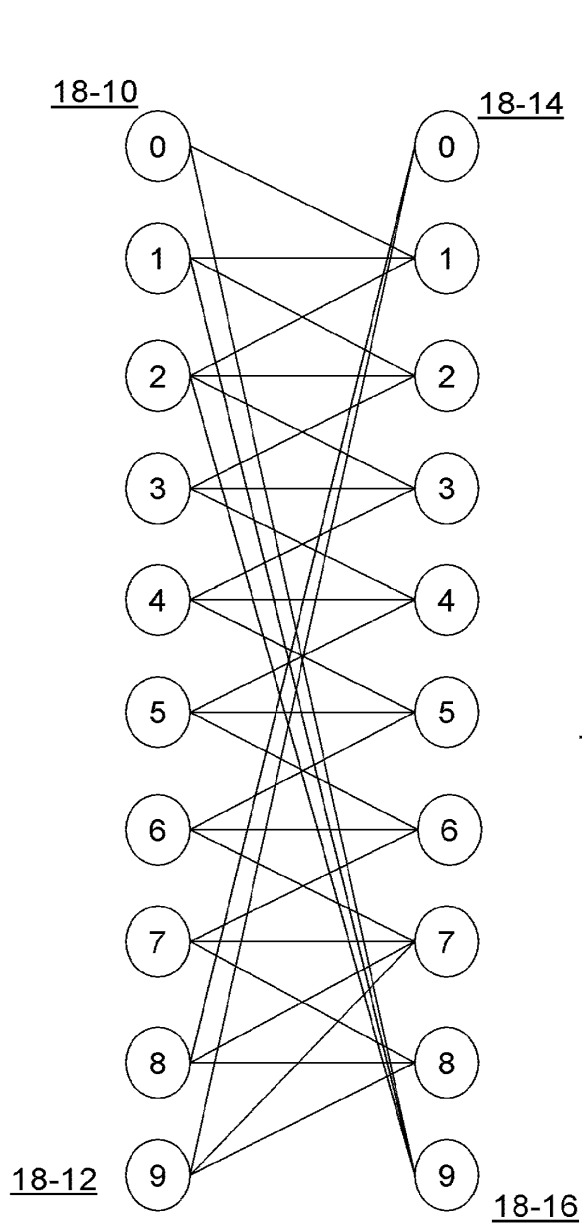


Figure 18

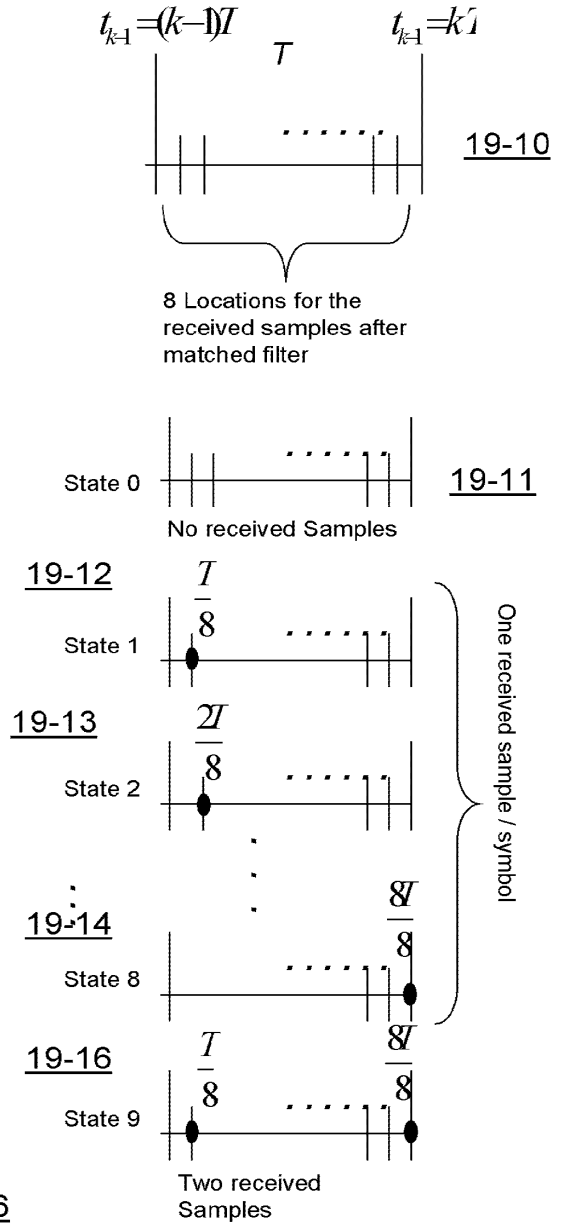
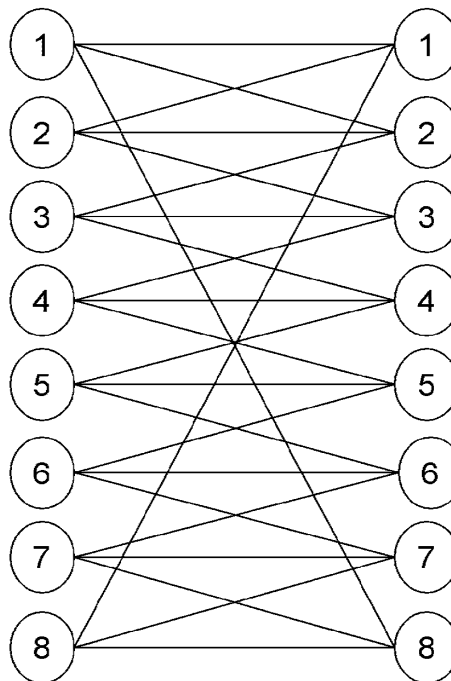
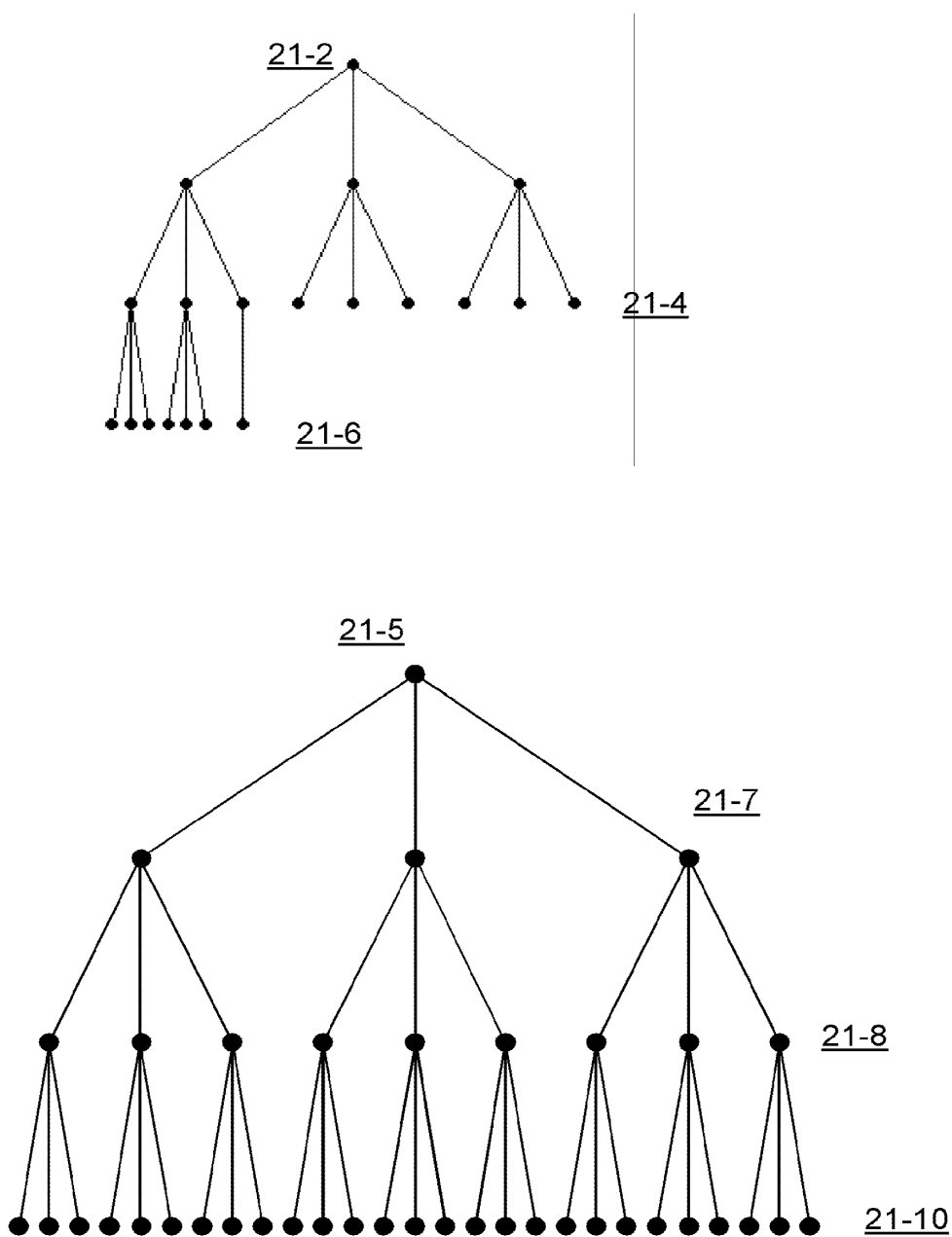
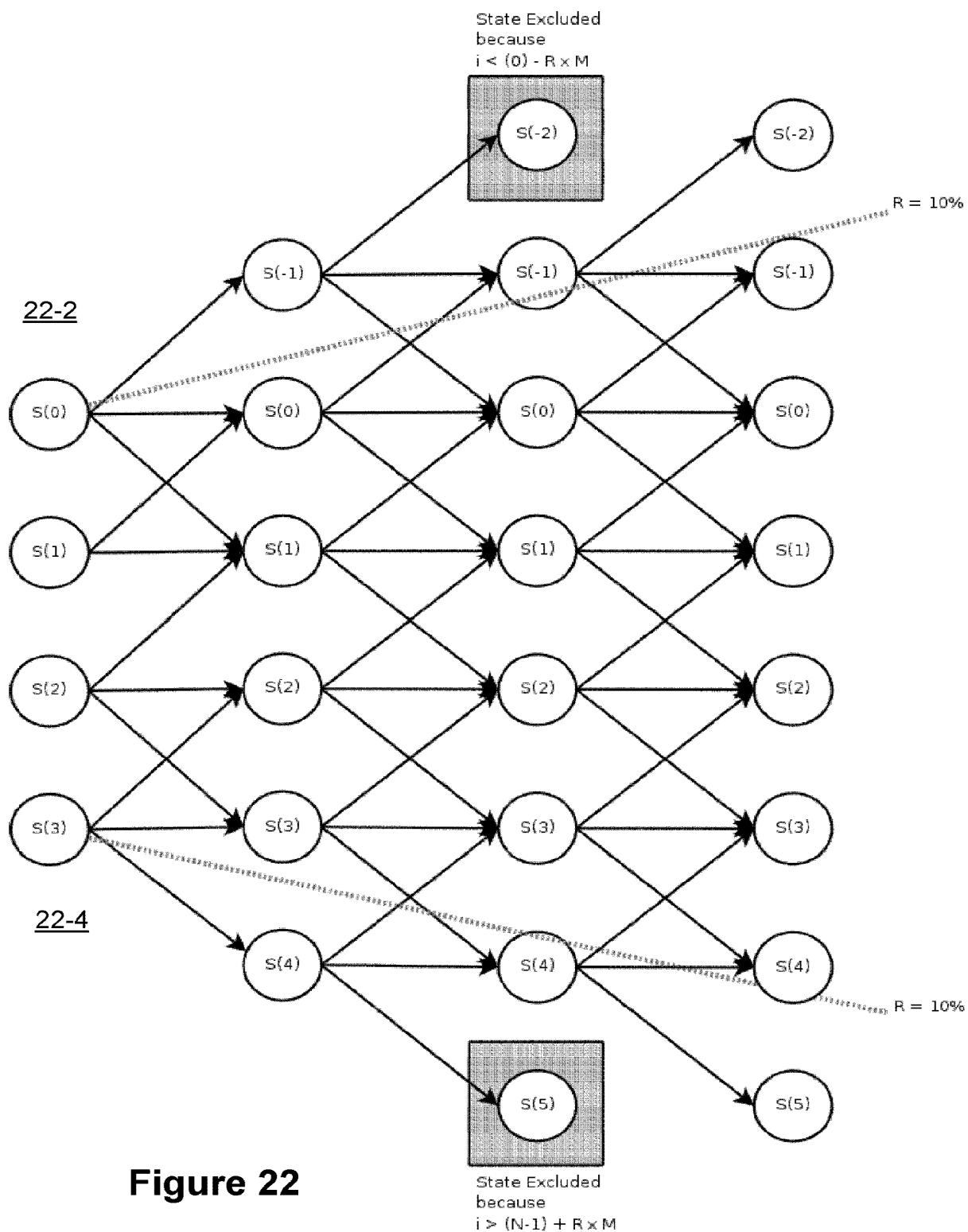


Figure 19

20-1020-1420-1220-16**Figure 20**

**Figure 21**

**Figure 22**

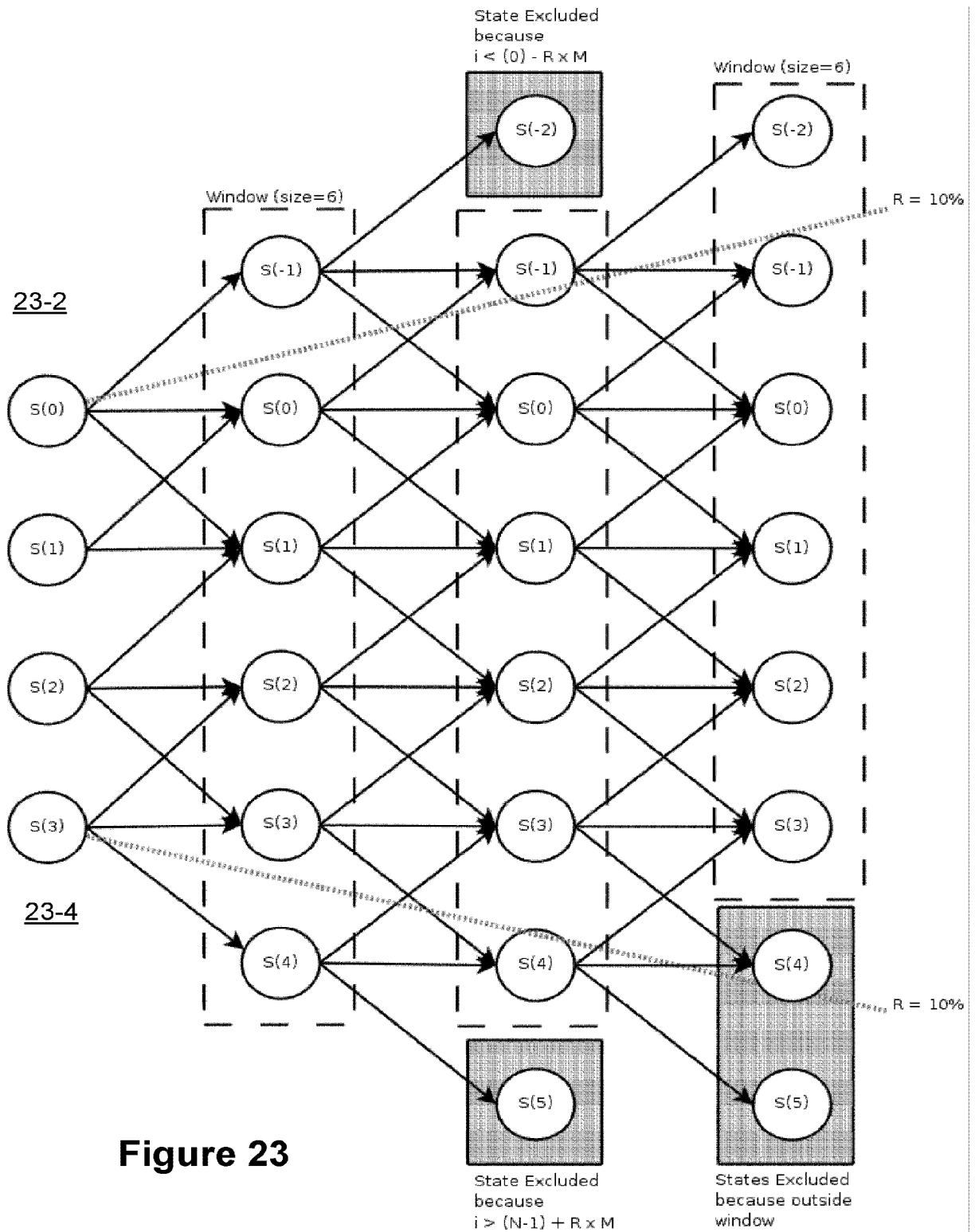
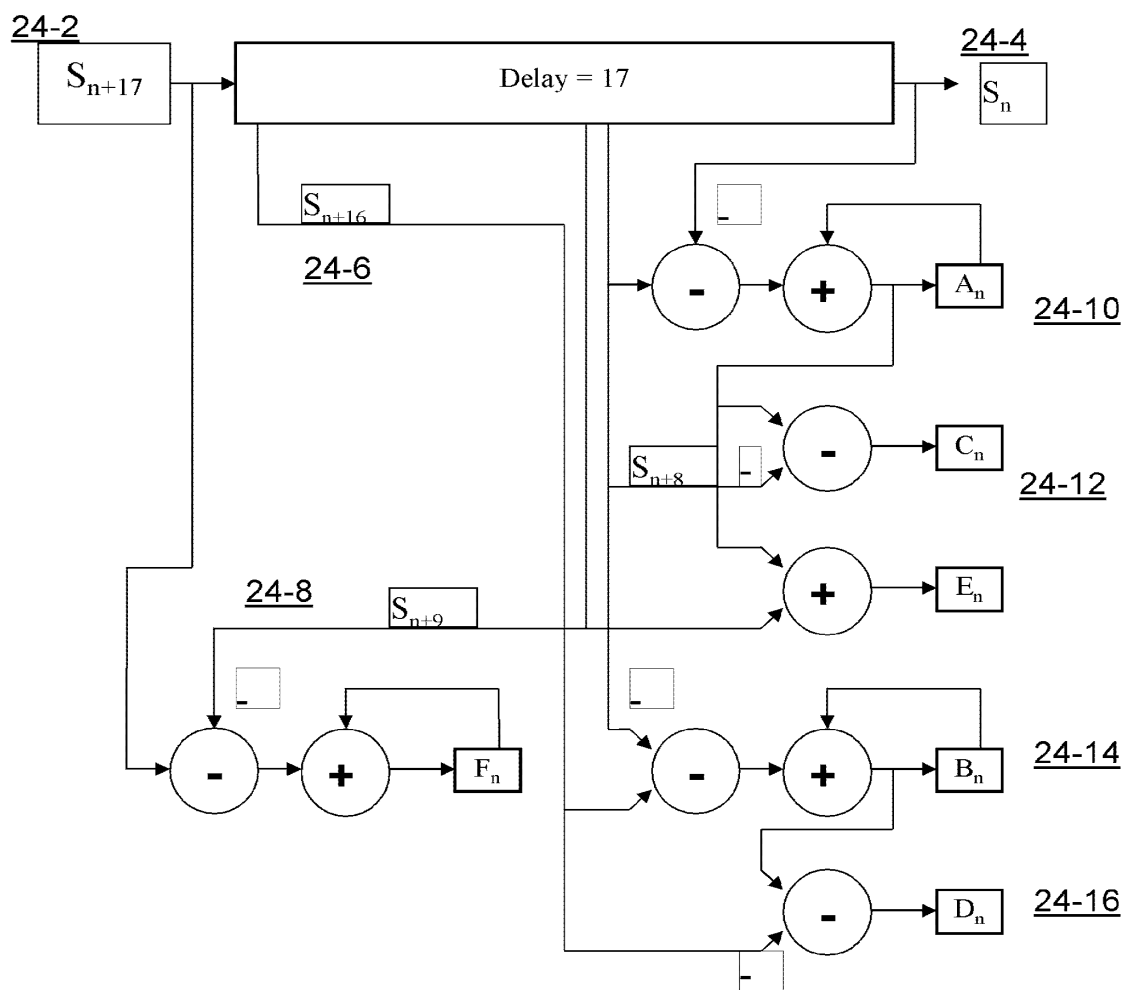
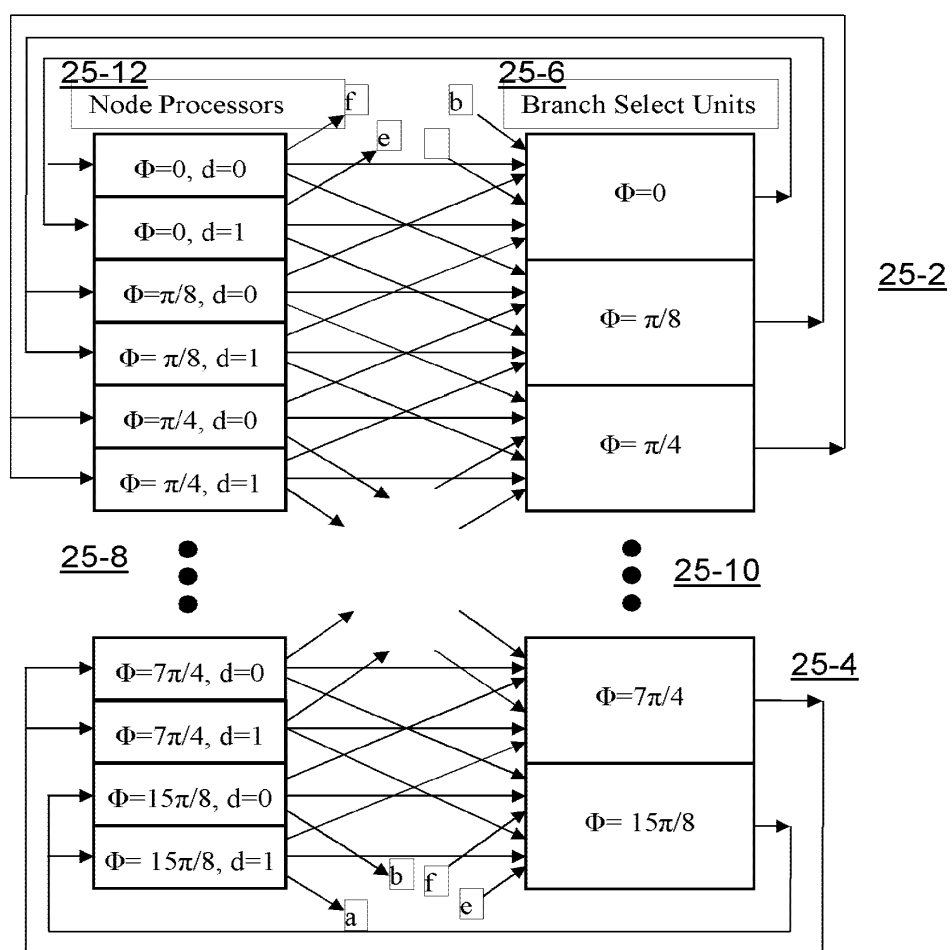


Figure 23

**Figure 24**

**Figure 25**

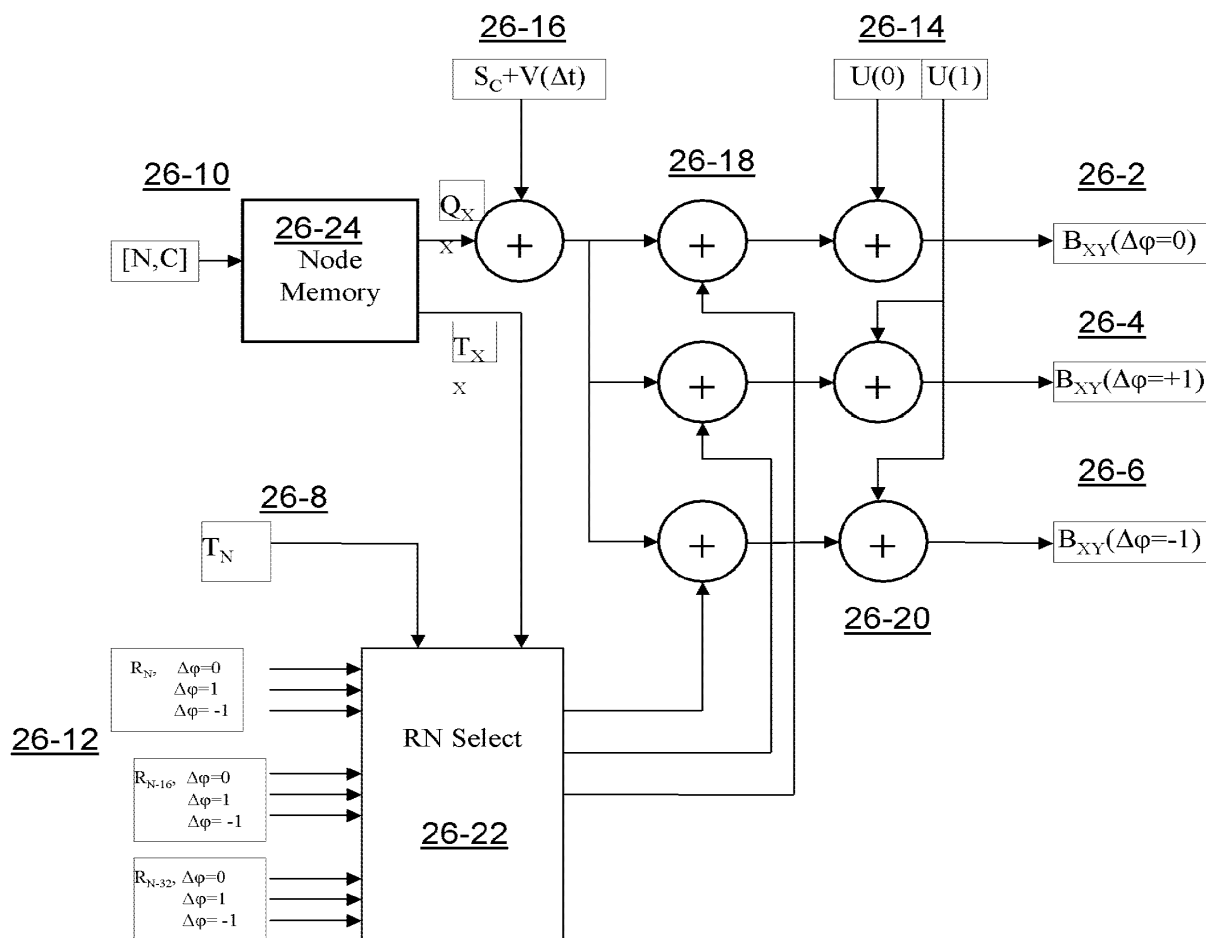


Figure 26

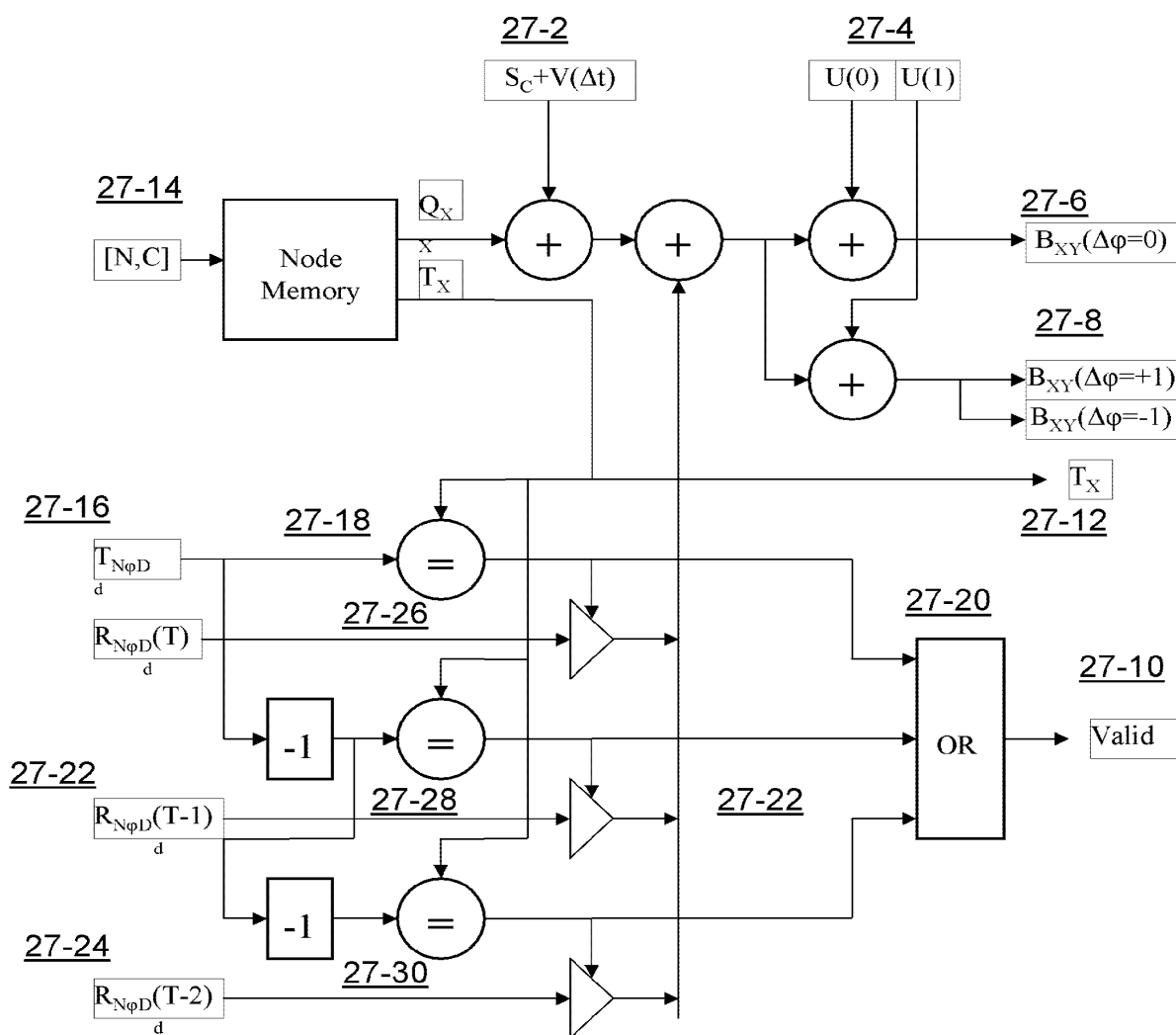


Figure 27

Electronic Patent Application Fee Transmittal				
Application Number:		12539431		
Filing Date:		11-Aug-2009		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Michael Davis		
Filer:		Matthew Ryan Ellsworth/Robert Roe-Pachirat		
Attorney Docket Number:		2943AAAB-178		
Filed as Large Entity				
Utility under 35 USC 111(a) 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:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt	
EFS ID:	14355639
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178
Receipt Date:	30-NOV-2012
Filing Date:	11-AUG-2009
Time Stamp:	16:02:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 180
RAM confirmation Number	3581
Deposit Account	191970
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_06.pdf	888927	yes	8
			dae06feb3b8cc551eb8449abf888d09412027b9e		
	Multipart Description/PDF files in .zip description				
	Document Description	Start	End		
	Transmittal Letter	1	3		
	Information Disclosure Statement (IDS) Form (SB08)	4	8		
Warnings:					
Information:					
2	Foreign Reference	CN1307309.pdf	693358	no	18
			65f9ce0d3b0ee549a76c32d4da8e12efef63388e		
Warnings:					
Information:					
3	Foreign Reference	EP0956818.pdf	945505	no	21
			a7d046f8c834dd0933c6377431308b8f8dc8c4f89		
Warnings:					
Information:					
4	Foreign Reference	EP1251448.pdf	1487814	no	23
			5006753e4e46eb5943c6ec6e728aebcc2c14f84b		
Warnings:					
Information:					
5	Foreign Reference	GB2256170.pdf	285817	no	9
			9cf37c40f770b0857849f88e401bb40833632026		
Warnings:					
Information:					
6	Foreign Reference	GB2331825.pdf	835999	no	22
			69e55d96f8c0b487ffc7c41a5f8fc4fb5b79b819		
Warnings:					
Information:					
7	Foreign Reference	JP2002261749.pdf	749773	no	13
			b7a252d9d015fcd24d2a835a285dcc99d91aeb13		
Warnings:					
Information:					

8	Foreign Reference	KR2002-0073716.pdf	524543	no	11
			2a3c5950122800874eab6544c476d3d55b6aa885		
Warnings:					
Information:					
9	Foreign Reference	RU2158444.pdf	1182866	no	15
			6247b83afc1746ac1097113cecb24a73a5482dfb		
Warnings:					
Information:					
10	Foreign Reference	RU2195020.pdf	675526	no	10
			7df8dada4a66f177e69482b8500dfd644a572f58		
Warnings:					
Information:					
11	Foreign Reference	WO9717683.pdf	1275616	no	28
			4c7875aacccaf85dbbb506b31a8615392e90e3e5		
Warnings:					
Information:					
12	Foreign Reference	WO9956429.pdf	2058882	no	49
			8ded1ae942f1d14bf3519ca2f67adc4d69cebdf		
Warnings:					
Information:					
13	Foreign Reference	WO0113218.pdf	901679	no	24
			2cf8b2c7435670c869a55c241dd9340db64729f0		
Warnings:					
Information:					
14	Foreign Reference	WO2004010373.pdf	1573669	no	38
			33c787c600b1ad38ae5827de8f2bbf0bd6836d59		
Warnings:					
Information:					
15	Foreign Reference	WO2005001777.pdf	465022	no	12
			70fb54f7602a2d11e7c51962a6b3ab27d1c7f939		
Warnings:					
Information:					
16	Foreign Reference	WO2006123316.pdf	951766	no	21
			e550317e290de2c2c47d8eda7492bb8ff9e41b0		
Warnings:					
Information:					

17	Foreign Reference	WO2007094868.pdf	3889794 d00c1cf6fcbf3447e6529a4f707987b91626 eea	no	76
Warnings:					
Information:					
18	Fee Worksheet (SB06)	fee-info.pdf	30576 038cfd3847013d3d4a6e6fc1b794fb9d87d d7a8	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			19417132		
<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>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
Michael Davis	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Cordelia P.K. Zecher
Filed: August 11, 2009	)	
Atty. File No.: 2943AAAB-178	)	<u>SUPPLEMENTAL</u>
Entitled: "Secure Wiegand Communications"	)	<u>INFORMATION DISCLOSURE</u>
	)	<u>STATEMENT</u>
	)	<i>Electronically Submitted</i>

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

- ☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.
- ☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.
- ☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.
- ☒ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.
- ☒ Examiner's attention is drawn to the following related applications:
 - Serial No. 12/002,145 filed 12/14/2007 (Attorney Ref. No. 2943AAAB-227)
- ☐ Other: _____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☐	<p>37 CFR 1.97(b): No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction):</p> <div style="margin-left: 20px;"> ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or ☐ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. </div> <p>Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.</p>
☐	<p>37 CFR 1.97(c): The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions:</p> <div style="margin-left: 20px;"> (1) a final action under 37 C.F.R. 1.113, or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. </div> <p>This Information Disclosure Statement is accompanied by:</p> <div style="margin-left: 20px;"> ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. <div style="text-align: center;">OR</div> ☐ Please charge Deposit Account 19-1970 in the amount of \$180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. </div>
☒	<p>37 CFR 1.97(d): This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c).</p> <div style="margin-left: 20px;"> ☒ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) <div style="text-align: center;">AND</div> ☒ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of \$180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification. </div>

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)



The undersigned certifies that:



Each item of information contained in this 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 this statement. 37 C.F.R. 1.97(e)(1).



A copy of the communication from the foreign patent office is enclosed.

OR



No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By:



Matthew R. Ellsworth

Registration No. 56345

1560 Broadway, Suite 1200

Denver, Colorado 80202-5141

(303) 863-9700

Date: November 30, 2012

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **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)

22442 7590 08/31/2012
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

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.

Leslie M. Roberts	(Depositor's name)
/Leslie M. Roberts/	(Signature)
November 30, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292
------------	------------	---------------	--------------	------

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	11/30/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
ZECHER, CORDELIA P K	2432	380-262000

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, 1 Sheridan Ross P.C.
- (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. 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)

Assa Abloy AB

Sweden

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. X Payment made
- ☐ Payment by credit card. Form PTO-2038 is attached. via EFS-Web
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Matthew R. Ellsworth/

Date November 30, 2012

Typed or printed name Matthew R. Ellsworth

Registration No. 56,345

This collection of information 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.

Electronic Patent Application Fee Transmittal				
Application Number:		12539431		
Filing Date:		11-Aug-2009		
Title of Invention:		SECURE WIEGAND COMMUNICATIONS		
First Named Inventor/Applicant Name:		Michael Davis		
Filer:		Matthew Ryan Ellsworth/Leslie Roberts		
Attorney Docket Number:		2943AAAB-178		
Filed as Large Entity				
Utility under 35 USC 111(a) 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:				
Utility Appl issue fee	1501	1	1770	1770
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2070

Electronic Acknowledgement Receipt	
EFS ID:	14359732
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178
Receipt Date:	30-NOV-2012
Filing Date:	11-AUG-2009
Time Stamp:	18:48:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 2070
RAM confirmation Number	7986
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
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)	ISSUE_FEE.pdf	89886	no	1
			407b6a3ac30e44a7d020caeb6dba7878247921c8		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32050	no	2
			803371cd0fab4d8ec7c1b9260761aca81d104907		
Warnings:					
Information:					
Total Files Size (in bytes):			121936		
<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>					

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
				Attorney Docket Number	2943AAAB-178
Sheet	1	of	5		

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3842350	10/15/1974	Gross	
	2	4163215	07/31/1979	Iida	
	3	4333072	06/01/1982	Beigel	
	4	4425645	01/10/1984	Weaver et al.	
	5	4519068	05/21/1985	Krebs et al.	
	6	4549264	10/22/1985	Carroll et al.	
	7	4656463	04/07/1987	Anders et al.	
	8	4688026	08/18/1987	Scribner et al.	
	9	4849927	07/18/1989	Vos	
	10	5013898	05/07/1991	Glasspool	
	11	5028918	07/02/1991	Giles et al.	
	12	5041826	08/20/1991	Milheiser	
	13	5050150	09/17/1991	Ikeda	
	14	5151684	09/29/1992	Johnsen	
	15	5166676	11/24/1992	Milheiser	
	16	5218344	06/08/1993	Ricketts	
	17	5235642	08/10/1993	Wobber et al.	
	18	5343469	08/30/1994	Ohshima	
	19	5347263	09/13/1994	Carroll et al.	
	20	5396215	03/07/1995	Hinkle	
	21	5426425	06/20/1995	Comad et al.	
	22	5467082	11/14/1995	Sanderson	
	23	5491471	02/13/1996	Stobbe	
	24	5517172	05/14/1996	Chiu	
	25	5519381	05/21/1996	Marsh et al.	
	26	5521602	05/28/1996	Carroll et al.	
	27	5594384	01/14/1997	Carroll et al.	
	28	5600683	02/04/1997	Bierach et al.	
	29	5679945	10/21/1997	Renner et al.	
	30	5724417	03/03/1998	Bartholomew et al.	
	31	5745037	04/28/1998	Guthrie et al.	
	32	5777561	07/07/1998	Chieu et al.	
Examiner Signature	/Cordelia Zecher/			Date Considered	12/06/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	2	of	5	Attorney Docket Number	2943AAAB-178

	33	5848541	12/15/1998	Glick et al.	
	34	5886894	03/23/1999	Rakoff	
	35	5887176	03/23/1999	Griffith et al.	
	36	5909462	06/01/1999	Kamerman et al.	
	37	5923264	07/13/1999	Lavelle et al.	
	38	5929779	07/27/1999	MacLellan et al.	
	39	5952922	09/14/1999	Shober	
	40	5952935	09/14/1999	Mejia et al.	
	41	5954583	09/21/1999	Green	
	42	5991410	11/23/1999	Albert et al.	
	43	5995956	11/30/1999	Nguyen	
	44	6078251	06/20/2000	Landt et al.	
	45	6182214	01/30/2001	Hardjono	
	46	6192222	02/20/2001	Greeff et al.	
	47	6212175	04/03/2001	Harsch	
	48	6219439	04/17/2001	Burger	
	49	6223984	05/01/2001	Renner et al.	
	50	6249212	06/19/2001	Beigel et al.	
	51	6259367	07/10/2001	Klein	
	52	6272562	08/07/2001	Scott et al.	
	53	6285681	09/04/2001	Kolze et al.	
	54	6304613	10/16/2001	Koller et al.	
	55	6307517	10/23/2001	Lee	
	56	6317027	11/13/2001	Watkins	
	57	6325285	12/04/2001	Baratelli	
	58	6366967	04/02/2002	Wagner	
	59	6377176	04/23/2002	Lee	
	60	6420961	07/16/2002	Bates et al.	
	61	6483427	11/19/2002	Werb	
	62	6496595	12/17/2002	Puchek et al.	
	63	6496806	12/17/2002	Horwitz et al.	
	64	6509828	01/21/2003	Bolavage et al.	
	65	6617962	09/09/2003	Horwitz et al.	
	66	6677852	01/13/2004	Landt	
	67	6717516	04/06/2004	Bridgelall	
	68	6903656	06/07/2005	Lee	
Examiner Signature	/Cordelia Zecher/			Date Considered	12/06/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	3	of	5	Attorney Docket Number	2943AAAB-178

	69	6922558	07/26/2005	Delp et al.	
	70	6963270	11/08/2005	Gallagher, III et al.	
	71	6992567	01/31/2006	Cole et al.	
	72	7026935	04/11/2006	Diorio et al.	
	73	7197279	03/27/2007	Bellantoni	
	74	7268681	09/11/2007	Fitzgibbon	
	75	7269416	09/11/2007	Guthrie et al.	
	76	7375616	05/20/2008	Rowse et al.	
	77	7378967	05/27/2008	Sullivan et al.	
	78	7551081	06/23/2009	Vrba et al.	
	79	2002/0036569	03/28/2002	Martin	
	80	2002/0131595	09/19/2002	Veda et al.	
	81	2003/0007473	01/09/2003	Strong et al.	
	82	2003/0055667	03/20/2003	Sgambaro et al.	
	83	2003/0081785	05/01/2003	Boneh et al.	
	84	2004/0069852	04/15/2004	Seppinen et al.	
	85	2004/0087273	05/06/2004	Pertti1a et al.	
	86	2004/0089707	05/13/2004	Cortina et al.	
	87	2004/0176032	09/09/2004	Kotola et al.	
	88	2004/0179684	09/16/2004	Appenzeller et al.	
	89	2004/0212493	10/28/2004	Stilp	
	90	2004/0232220	11/25/2004	Beenau et al.	
	91	2005/0010750	01/13/2005	Ward et al.	
	92	2005/0036620	02/17/2005	Casden et al.	
	93	2005/0063004	03/24/2005	Silverbrook et al.	
	94	2005/0116813	06/02/2005	Raskar	
	95	2005/0127172	06/16/2005	Merkert Sr.	
	96	2006/0101274	05/11/2006	Merkert et al.	
	97	2006/0156027	07/13/2006	Blake	
	98	2006/0181397	08/17/2006	Limbachiya	
	99	2006/0255129	11/16/2006	Griffiths	
	100	2006/0288101	12/21/2006	Mastrodonato et al.	
	101	2007/0273497	11/29/2007	Kuroda et al.	
	102	2008/0014867	01/17/2008	Finn	
	103	2008/0032626	02/07/2008	Chen	
	104	2008/0094171	04/24/2008	Sawhney	
Examiner Signature	/Cordelia Zecher/			Date Considered	12/06/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	4	of	5	Attorney Docket Number	2943AAAB-178

	105	2008/0229400	09/18/2008	Burke	
	106	2009/0315673	12/24/2009	Huang	
	107	2010/0001840	01/17/2010	Kang et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	108	CN 1307309	08/08/2001	BEIJING KERUIQI TECHNOLOGY DEV		(with English abstract)
	109	EP 0956818	11/17/1999	CITICORP DEV CENTER		
	110	EP 1251448	10/23/2002	TOO MNOGOPROFILNOE PREDPR		
	111	GB 2256170	12/02/1992	BRANDES WILLIAM ROBERT		
	112	GB 2331825	06/02/1999	NEC CORP		
	113	JP 2002-261749	09/13/2002	MATSUSHITA ELECTRIC IND CO LTD		(with English abstract)
	114	KR 2002-0073716	09/28/2002	FIRSTECH INT INC		(with English abstract)
	115	RU 2158444	10/27/2000	AJ DI SISTEMS INK		(with English abstract)
	116	RU 2195020	12/20/2002	MNOGOPROFIL NOE PRED OOO EHLSI		(with English abstract)
	117	WO 97/17683	05/15/1997	ID SYSTEMS INC		
	118	WO 99/56429	11/04/1999	IDENTIX INC		
	119	WO 01/13218	02/22/2001	SIEMENS AG		(with English Abstract)
	120	WO 2004/010373	01/29/2004	BANQUE TEC INTERNAT PTY LTD		
	121	WO 2005/001777	01/06/2005	SCM MICROSYSTEMS GMBH		

Examiner Signature	/Cordelia Zecher/	Date Considered	12/06/2012
--------------------	-------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	5	of	5	Attorney Docket Number	2943AAAB-178

	122	WO 2006/123316	11/23/2006	KONINKL PHILIPS ELECTRONICS NV		
	123	WO 2007/094868	08/23/2007	MOJIX INC		

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. ¹	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, page(s), volume-issue number(s), publisher, city and/or country where published.

Examiner Signature	/Cordelia Zecher/	Date Considered	12/06/2012
-----------------------	-------------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./



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.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292
22442	7590	12/10/2012		
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			EXAMINER ZECHER, CORDELIA P K	
			ART UNIT 2432	PAPER NUMBER
			MAIL DATE 12/10/2012	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.



UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
12/539,431	11 August, 2009	DAVIS ET AL.	2943AAAB-178

Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202		EXAMINER	
		CORDELIA ZECHER	
		ART UNIT	PAPER
		2432	20121206

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed on November 30, 2012 has been considered. However, due to the extensive nature of the IDS the references cited have been considered only by a cursory review.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

PTO-90C (Rev.04-03)

Receipt date: 02/24/2010

12539431 - GAU: 2432

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
				Attorney Docket Number	2943-178
Sheet	4	of	8		

105	2008/0184349	7/31/2008	Ting	
-----	--------------	-----------	------	--

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ ; Number ⁴ ; Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	106	AU 2006203768	3/15/07	Davis et al.		
	107	CA 2556843	2/28/07	Davis et al.		
	108	WO 01/013218	02/22/01	Siemens Aktiengesellschaft		(Translated Abstract Attached)
	109	WO 01/18331	03/15/01	Electec System Aktiebolag		
	110	WO 03/027832	04/03/03	Intel Corporation		
	111	WO 03/042812	05/22/03	Everbee Networks		(Translated Abstract Attached)
	112	WO 04/010373	01/29/04	Banque-Tec International Pty Ltd		
	113	WO 05/001777	01/06/05	SCM Microsystems GMBH		
	114	WO 2004/039119	05/06/04	Anzon Autodoor Limited		
	115	WO 2005/018137	02/24/05	Securicom Pty Ltd		
	116	WO 2005/029315	03/31/05	Globespanvirata Incorporated		
	117	WO 2005/038729	04/28/05	SCM Microsystems, Inc.		
	118	WO 2006/015625	06/09/04	Telecom Italia S.P.A.	2006-02-16	

Change(s) applied
to document,

/M.H.E./

10/2/2009

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012
-----------------------	-------------------	--------------------	------------

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 11/30/2012

12539431 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	3	of	5	Attorney Docket Number	2943AAAB-178

	69	6922558	07/26/2005	Delp et al.	
	70	6963270	11/08/2005	Gallagher, III et al.	
	71	6992567	01/31/2006	Cole et al.	
	72	7026935	04/11/2006	Diorio et al.	
	73	7197279	03/27/2007	Bellantoni	
	74	7268681	09/11/2007	Fitzgibbon	
	75	7269416	09/11/2007	Guthrie et al.	
	76	7375616	05/20/2008	Rowse et al.	
	77	7378967	05/27/2008	Sullivan et al.	
	78	7551081	06/23/2009	Vrba et al.	
	79	2002/0036569	03/28/2002	Martin	
	80	2002/0131595	09/19/2002	Veda et al.	
	81	2003/0007473	01/09/2003	Strong et al.	
	82	2003/0055667	03/20/2003	Sgambaro et al.	
	83	2003/0081785	05/01/2003	Boneh et al.	
	84	2004/0069852	04/15/2004	Seppinen et al.	
	85	2004/0087273	05/06/2004	Perttinen et al.	Perttinen
	86	2004/0089707	05/13/2004	Cortina et al.	
	87	2004/0176032	09/09/2004	Kotola et al.	
	88	2004/0179684	09/16/2004	Appenzeller et al.	
	89	2004/0212493	10/28/2004	Stilp	
	90	2004/0232220	11/25/2004	Beenau et al.	
	91	2005/0010750	01/13/2005	Ward et al.	
	92	2005/0036620	02/17/2005	Casden et al.	
	93	2005/0063004	03/24/2005	Silverbrook et al.	
	94	2005/0116813	06/02/2005	Raskar	
	95	2005/0127172	06/16/2005	Merkert Sr.	
	96	2006/0101274	05/11/2006	Merkert et al.	
	97	2006/0156027	07/13/2006	Blake	
	98	2006/0181397	08/17/2006	Limbachiya	
	99	2006/0255129	11/16/2006	Griffiths	
	100	2006/0288101	12/21/2006	Mastrodonato et al.	
	101	2007/0273497	11/29/2007	Kuroda et al.	
	102	2008/0014867	01/17/2008	Finn	
	103	2008/0032626	02/07/2008	Chen	
	104	2008/0094171	04/24/2008	Sawhney	
Examiner Signature	/Cordelia Zecher/			Date Considered	12/06/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./



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.
12/539,431	01/22/2013	8358783	2943AAAB-178	9292

22442 7590 12/29/2012
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

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 594 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):

Michael Davis, Amherst, NY;
David Andresky, Lafayette, CO;
Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;

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.