

Exhibit 337–B: 35 U.S.C. § 103 References for U.S. Patent No. 9,667,337 Claims 1, 2, 3, 6, 8, 9, 11, 17, 26, 29, 30, 32, 33, 35, 48, and 49

To the extent Plaintiff contends that any particular prior art reference charted by Samsung lacks any feature, a person of ordinary skill in the art as of the '337 patent's purported invention date would, at a minimum, have been motivated to modify the reference to include the allegedly missing feature, or to combine it with other references that include that feature (as demonstrated in (a) Defendants' invalidity charts for other prior art references and/or (b) the chart below), as discussed in the cover document of Defendants' invalidity contentions.

The analysis in this chart is based on the Court's claim constructions and the apparent interpretations that Plaintiff has advanced to allege infringement of the asserted claims of the '337 patent, and Samsung's current understanding of the scope of the asserted claims associated therewith. Nothing in this chart should be interpreted as Samsung conceding that Plaintiff's interpretations are correct or supported by intrinsic or extrinsic evidence.

Further, as set forth in the cover document of Samsung's invalidity contentions, many of the claim terms in the asserted claims suffer from 35 U.S.C. § 112 issues, such as lack of written description, lack of enablement, and/or indefiniteness. Nothing in this chart should be taken as an admission or suggestion that the asserted claims meet the statutory requirements of 35 U.S.C. § 112.

Additionally, as set forth in the cover document of Samsung's invalidity contentions, many of the claim terms in the asserted claims suffer from 35 U.S.C. § 101 issues because they are not directed to patent-eligible subject matter. Nothing in this chart should be taken as an admission or suggestion that the asserted claims meet the statutory requirements of 35 U.S.C. § 101. For example, where Samsung has identified prior art disclosures any claims directed to patent ineligible subject matter, Samsung's disclosure is made based on Samsung's understanding of Plaintiff's apparent interpretation of the claims, despite the claims being directed to an abstract idea and lacking an inventive concept to transform that abstract idea into patent eligible subject matter.

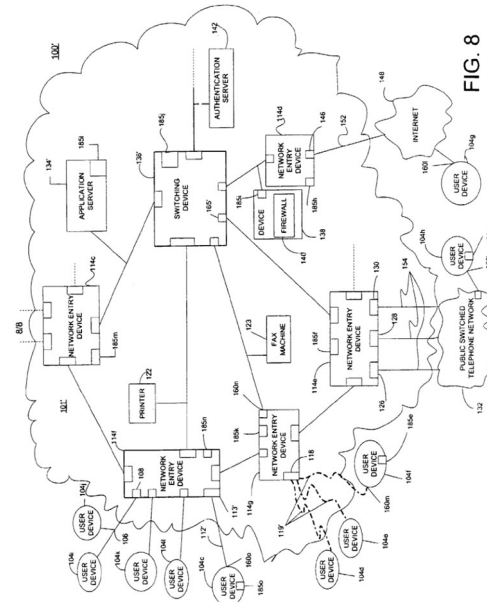
To the extent Plaintiff submits new infringement theories and/or identifies additional limitations of the asserted claims that they contend are not disclosed by the prior art references charted by Samsung, either alone or in combination with Samsung's other cited prior art, Samsung expressly reserves the right to rebut any such contention. The chart below provides representative examples of where additional prior art references disclose elements of the asserted claims, under Samsung's present understanding of those claims and/or under the apparent application of the claims that Plaintiff applied in its infringement contentions. The cited evidence is merely illustrative, and Samsung reserves the right to cite alternative or additional evidence. Where the chart below states that any reference "discloses" a limitation, such disclosure may be express or inherent. Samsung also intends to offer expert testimony and opinions establishing the general knowledge of a person of ordinary skill in the art (POSITA), known design objectives, motivations to combine references and elements within the general knowledge of a POSITA, the state-of-the-art, how a POSITA would understand the disclosures of the cited prior art references, and any secondary considerations/objective indicia identified by Plaintiff.

Claims	Prior Art
1[pre]. A broadband wireless repeater or relay, comprising:	"A broadband wireless repeater or relay" was well known at the time of the alleged invention. A person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include the claimed elements as set forth below and in Defendants' other invalidity charts. For example: See, e.g.:

Claims	Prior Art
	337-A01 U.S. Pat. No. 6,584,080 (“Ganz ’080”) 337-A02 U.S. Pat. Pub. No. 2002/0028655 (“Rosener ’655”) 337-A03 U.S. Pat. Pub. No. 2004/0160928 (“Perlman ’928”) 337-A04 U.S. Pat. No. 6,188,496 (“Krishna ’496”) 337-A05 U.S. Pat. No. 7,209,523 (“Larrick ’523”) 337-A06 U.S. Pat. No. 4,056,780 (“Faulkner ’780”) 337-A07 U.S. Pat. No. 6,497,656 (“Evans ’656”) 337-A08 U.S. Pat. Pub. No. 2003/0120809 (“Bellur ’809”) 337-A09 U.S. Pat. No. 8,125,940 (“Perlman ’940”) 337-A10 U.S. Pat. Pub. No. 2005/0201326 (“Lakkis ’326”) 337-A11 U.S. Pat. Pub. No. 2004/0048574 (“Walker ’574”) 337-A12 XtremeSpectrum Trinity Chipset Engels ’850 at Abstract An indoor to outdoor unit is described for placement outside of a building and adjacent to a structural part of the building. The unit has first antenna means (12) for communication with at least one indoor antenna (13) placed inside said building, the first antenna means having a reflector for reflecting radio signals towards the inside of the building. For instance, the first antenna means may be adapted to be located with respect to a wall of the building in such a way that a part of the wall is situated in the near-field region of the first antenna means. The first antenna means may be adapted for connection to a cable network. Alternatively; the unit may also have a second antenna means (10) for communication with at least one outdoor antenna (9) located outside the building. The first and second antenna means are adapted for attachment to or located in a housing. In operation some signals received by the second antenna means (10) from the one outdoor antenna (9) are transmitted to the first antenna means (12) and some signals transmitted from the second antenna means (10) to the one outdoor antenna (9) are received from the first antenna means (12) so that the unit acts as a repeater. Engels ’850 at 2:13–22 A known solution to this problem is the insertion of a repeater in the radio link, as depicted in Fig. 3: the information is first transmitted from the transmitting antenna (1) to an auxiliary receiving antenna (4)

Claims	Prior Art
	associated with the repeater. In a second step, the repeater amplifies the received signal and re-transmits it from an auxiliary transmitting antenna (5) associated with the repeater, to the receiving antenna (2). The resulting capacity of the link is then given by expression 3: [Equation 3] where gain is the signal gain of the repeater, and Attenuation 1 and Attenuation 2 are the signal attenuations over the two radio links, respectively. Engels '850 at 5:29 Fig. 3 shows a radio communications channel with repeater in side view. Engels '850 at 7:17–30 A first aspect of the present invention provides a solution for indoor coverage for a wireless radio communications network by placing an indoor to outdoor coupling unit (10, 12) outside a structural part of a building such as the outer wall of the building, as shown in Fig. 5. To place the unit it is preferably portable, e.g. has a housing to which the antennas are attached or wherein they are included, as well as any electronics placed within the housing in a suitable sealed compartment required to control the environment inside the unit. The portable unit may be brought to site as a kit of parts that are there assembled and installed at the appropriate location. The unit may be battery powered or may have a suitable power connection, e.g. for connection to the mains or an optional solar cell battery charging system for keeping the batteries charged up. The indoor-outdoor device is preferably in the form of a self-contained unit that does not require an opening in the wall of the building, i.e. does not have two parts: an indoor antenna and an outdoor antenna with a connection there between which must pass through the wall. Engels '850 at 13:27–14:2 Such an indoor-outdoor unit could, for instance, be used for transmitting digital data information between an outdoor antenna (e.g. a base station or an outdoor cell extending repeater) and one or more in-door computers. Alternatively, the indoor-outdoor coupling unit could be used for transmitting digital voice information between an outdoor antenna (e.g. a base station or an outdoor cell extending repeater) and an in-door telephony device or telephony network. Alternatively, the indoor-outdoor coupling unit could be used to communicate other forms of speech information, e.g. VOIP, or video information, such as e.g. Video-on-Demand or to provide connection to the Internet.

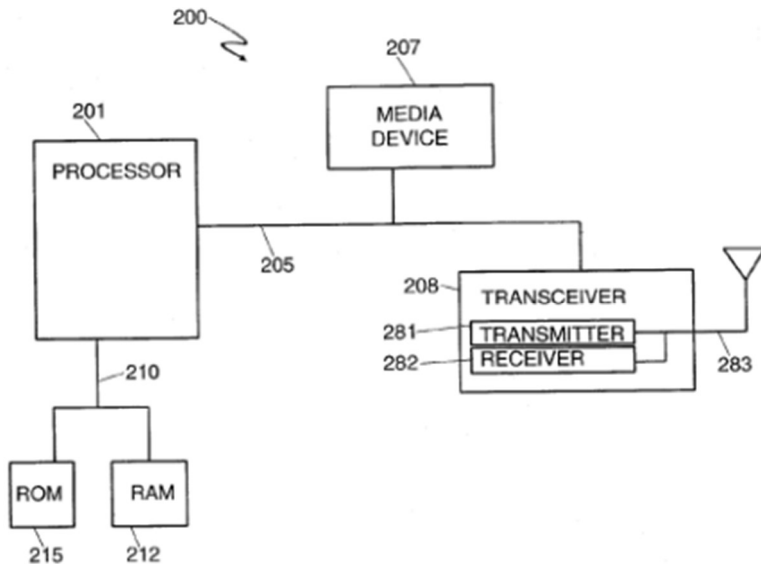
Claims	Prior Art
	Bareis '373 at Abstract Broadband multi-drop local network, interface and method for multimedia access. A local network architecture include a wired bus coupleable directly to an external data network terminal and configured for carrying broadband packetized data traffic over a frequency spectrum uninterrupted by other defined data channels or services; and one or a plurality of network transceivers operable individually for coupling an addressable network device processing a defined class of information to the bus wherein each network appliance is configured for and further operable for providing communication interfacing of the class of information of each addressable network appliance with the packetized IP data traffic on the wired bus. Roese '556 at Abstract A method for location discovery in a data network includes receiving, at a first device, connection information from a neighboring network device and determining a physical location of the first device based on the connection information. The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device be one of a variety of devices, such as a router, a switch, a network entry device, a firewall device, or a gateway.

Claims	Prior Art
	Roese '556 at FIG. 8  Roese '556 at 31:31–48 Network entry devices 114 and end user devices 104 can come in a wide array of configurations. For example, user devices 104 can include individual computers, printers, servers, cellular phones, laptops, handheld electronic devices, telephones, Internet Protocol (IP)-configured telephones, switch devices, and the like. Network entry devices 114 can include, for example, switches, routers, hubs, bridges, repeaters, wireless access points, data communications equipment, server computers, modems, multiplexers, Private Branch Exchanges (PBXs), virtually any devices used to interconnect data equipment or end devices, and the like. The discreet boundaries of infrastructure 101' are for illustration only. For example, system 100' may include a server outside of the illustrated boundary while remaining logically part of infrastructure 101'. In another example, there may be a portion of network infrastructure 101' connected to system 100' located in a remote network, such as Internet 148. Mandke 2003A at 5 TG3a has set out to develop a flexible standard which will enable high data rate WPAN (110 Mbps at 10m, 200 Mbps at 4m, and 480 Mbps at an unspecified distance) over a cost effective architecture. This new standard will enable a broad range of applications including the wireless transmission of images and

Claims	Prior Art																												
	video. The goal of this paper is to explore the unique design issues specific to UWB, engineering trade-offs faced by standards developers, and the current state of IEEE 802.15.3a. Section 2 will discuss the unique aspects of indoor UWB channels and the four of the proposed TG3a channel models. Section 3 compares a traditional impulse radio approach to UWB with a more recent multibanded approach (which has been employed in many TG3a proposals). Section 4 details the requirements and specifications set forth by IEEE 802.15.3a, and categorize the proposals being considered in order to form a clear picture of the current state of UWB technology as it relates to WPANs. Mandke 2003A at Page 24 <table border="1"> <thead> <tr> <th>Company</th><th>Texas Instruments</th></tr> </thead> <tbody> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>3 (additional bands can be added in the future)</td></tr> <tr> <td>Bandwidths</td><td>503.25 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.168 GHz – 4.752 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>TFI-OFDM, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>not available</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>312.5 ns OFDM symbol</td></tr> <tr> <td>Multipath mitigation method</td><td>1-tap (robust to 60.6 ns delay spread)</td></tr> </tbody> </table> A. Batra, et. al. "TI Physical Layer Proposal for IEEE 802.15 Task Group 3a," IEEE P802.15-03/142r0. March 3, 2003.	Company	Texas Instruments	Spectrum Allocation:		# of bands	3 (additional bands can be added in the future)	Bandwidths	503.25 MHz	Frequency ranges	3.168 GHz – 4.752 GHz	Modulation Scheme	TFI-OFDM, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	not available	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps	Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps	Symbol period	312.5 ns OFDM symbol	Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)
Company	Texas Instruments																												
Spectrum Allocation:																													
# of bands	3 (additional bands can be added in the future)																												
Bandwidths	503.25 MHz																												
Frequency ranges	3.168 GHz – 4.752 GHz																												
Modulation Scheme	TFI-OFDM, QPSK																												
Coexistence method	null band for WLAN (~5 GHz)																												
Multiple access method	not available																												
# of simultaneous piconets	not available																												
Error correction codes	Convolutional code																												
Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps																												
Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps																												
Symbol period	312.5 ns OFDM symbol																												
Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)																												

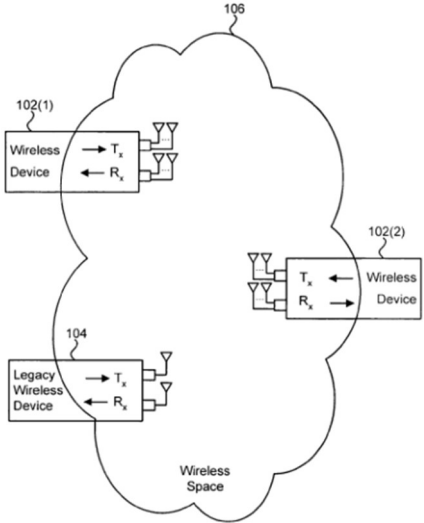
Claims	Prior Art																																																								
	Mandke 2003A at Page 24 <table border="1"> <tr> <th>Company</th><th>XtremeSpectrum</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>2</td></tr> <tr> <td>Bandwidths</td><td>1.368 GHz, 2.736 GHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>BPSK, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Ternary CDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>4 piconets/band</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Soloman code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps</td></tr> <tr> <td>Chip duration</td><td>731 ps (Low band), 365.5 ps (High band)</td></tr> <tr> <td>Multipath mitigation method</td><td>Decision feedback equalizer</td></tr> </table> R. Roberts, “XtremeSpectrum CFP Document,” IEEE P802.15-03/154r1. March 3, 2003. Mandke 2003A at Page 27 <table border="1"> <tr> <th>Company</th><th>Discrete Time</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>15 bands</td></tr> <tr> <td>Bandwidths</td><td>500 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 10.6 GHz,</td></tr> <tr> <td>Modulation Scheme</td><td>QPSK, FH</td></tr> <tr> <td>Coexistence method</td><td>sacrifice 2 band for WLAN coexistence (5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>FDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps</td></tr> <tr> <td>Link margin</td><td>15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps</td></tr> <tr> <td>Multipath mitigation method</td><td>not available</td></tr> </table> Roberto Aiello, “Discrete Time PHY Proposal for TG3a,” IEEE 802.15-03/099r1. March 2003.	Company	XtremeSpectrum	Spectrum Allocation:		# of bands	2	Bandwidths	1.368 GHz, 2.736 GHz	Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz	Modulation Scheme	BPSK, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	Ternary CDMA	# of simultaneous piconets	4 piconets/band	Error correction codes	Convolutional code, Reed-Soloman code	Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps	Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps	Chip duration	731 ps (Low band), 365.5 ps (High band)	Multipath mitigation method	Decision feedback equalizer	Company	Discrete Time	Spectrum Allocation:		# of bands	15 bands	Bandwidths	500 MHz	Frequency ranges	3.1 GHz – 10.6 GHz,	Modulation Scheme	QPSK, FH	Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)	Multiple access method	FDMA	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	½ @ 110 Mbps	Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps	Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps	Multipath mitigation method	not available
Company	XtremeSpectrum																																																								
Spectrum Allocation:																																																									
# of bands	2																																																								
Bandwidths	1.368 GHz, 2.736 GHz																																																								
Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz																																																								
Modulation Scheme	BPSK, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	Ternary CDMA																																																								
# of simultaneous piconets	4 piconets/band																																																								
Error correction codes	Convolutional code, Reed-Soloman code																																																								
Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps																																																								
Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps																																																								
Chip duration	731 ps (Low band), 365.5 ps (High band)																																																								
Multipath mitigation method	Decision feedback equalizer																																																								
Company	Discrete Time																																																								
Spectrum Allocation:																																																									
# of bands	15 bands																																																								
Bandwidths	500 MHz																																																								
Frequency ranges	3.1 GHz – 10.6 GHz,																																																								
Modulation Scheme	QPSK, FH																																																								
Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)																																																								
Multiple access method	FDMA																																																								
# of simultaneous piconets	not available																																																								
Error correction codes	Convolutional code																																																								
Code rates	½ @ 110 Mbps																																																								
Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps																																																								
Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps																																																								
Multipath mitigation method	not available																																																								

Claims	Prior Art
	Fontana at 2 UWB APPLICATIONS Figure 1 illustrates an ultra wideband, handheld transceiver that was designed for full duplex voice and data transmission at rates of up to 128 kb/s (CVSD) and 115.2 kb/s (RS232). The radio has an operational center frequency in L-band (1.5 GHz) with an instantaneous bandwidth of 400 MHz (27% fractional BW). Peak power output from the UWB transceiver was measured at 2.0 Watts, with a resultant average power (worst case) of 640 μW. This results in a worst case power density of 1.6 pW/Hz. These units have a range of approximately 1 to 2 km (with small antennas shown and line-of-sight), and an extended range of 10 to 20 miles with small gain antennas. Fontana at Figure 1  Figure 1. Full Duplex UWB Handheld Transceivers. Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one radio to another via an intermediate repeater link.

Claims	Prior Art
	Fontana at Figure 6  Figure 6. UWB Wireless Intercom Communications System (WICS). Aiello '273 at Fig. 2  FIG. 2 Chabas '657 at Abstract This telecommunications device (21, 22 or 23) forms part of a system comprising base stations (10, 12). This system permits the devices forming it to relay information among them. It is proposed to provide the devices with a plurality of transceiver devices (RX1, RX2, . . . , RXm, TX1, TX2, . . . , TXn) for exchanging information with other devices and/or base stations. Application: ODMA mobile radios

Claims	Prior Art
	Chabas '657 at [0001] The invention relates to a telecommunications device for a system comprising at least a base station and a plurality of secondary stations including circuits for relaying the information among them. Soomro '456 at [0008] To address the above-discussed deficiencies of the prior art, it is a primary object of the present invention to provide, for use in an independent basic service set (IBSS) network, a dynamic frequency selection (DFS) process enabled by a DFS element within beacon and probe response frames defining a DFS owner, a DFS interval specifying the time until channel switch in beacon intervals, a DFS count specifying a time in beacon intervals until the dynamic frequency selection owner initiates selection of the next operating channel frequency from the supported channel set, and a DFS recovery interval specifying a time after the end of the DFS interval when recovery procedures are initiated if no channel switch information was received during the past DFS interval. Channel switch information is presented in beacons following the end of the channel selection process, and within beacons during the DFS recovery interval. Melick '146 at 8:11–16 According to one aspect of the present invention, the present invention provides for storing data by persistently maintaining the data on a network, through retransmission. The data can be associated with expiration properties. The expiration properties can include geographical information and/or time attributes. The data can be in packets or streams.

Claims	Prior Art
	802-15-3a at PAR Form, Page 2 The intent of this project is to provide a standard for a low complexity, low cost, low power consumption alternate PHY for 802.15.3 (comparable to the goals for 802.15.3). The data rate will be high enough, 110 Mb/s or more (see 13a), to satisfy an evolutionary set of consumer multi-media industry needs for WPAN communications. The project will address the requirements to support multimedia data types in multiple compliant co-located systems and also coexistence (13b). 14. Intellectual Property: Sponsor has reviewed the IEEE patent policy with the working group? Yes Sponsor is aware of copyrights relevant to this project? No Sponsor is aware of trademarks relevant to this project? No Sponsor is aware of possible registration of objects or numbers due to this project? No 15. Are you aware of other standards or projects with a similar scope? No Similar Scope Project Information: 16. Is there potential for this standard (in part or in whole) to be submitted to an international organization for review/adoption?: Do not Know If yes, please answer the following questions: Which International Organization/Committee? International Contact Information? 17. Will this project focus on Health, Safety or Environmental Issues? No 18. Additional Explanatory Notes: (Item Number and Explanation) 13a) The CFAs responses collected by study group 802.15 SG3a over the past several months indicate an evolutionary market developing for a group of applications that will not be addressed by 802.15.3. For example, high data rates, at least 110 Mb/s, will be required for simultaneous time dependent applications such as multiple HDTV video streams without sacrificing the requirements for low complexity, low cost, and low power consumption. In addition to at least 110 Mbps data rate, additional data rates, both lower and higher, may be supported. 13b) It is in the best interest of users and the industry to strive for a level of coexistence with other wireless systems, especially those in similar market spaces. Coexistence requirements will be established in SG3a selection criteria against which the proposals will be evaluated. Gardner '709 at Abstract A modified preamble is used by extended devices that operate at higher rates, MIMO or other extensions relative to strict 802.11a-compliant devices. The extended devices might use multiple antenna techniques (MIMO), where multiple data streams are multiplexed spatially and/or multi-channel techniques, where an extended transmitter transmits using more than one 802.11a channel at a time. Such extensions to IEEE 802.11a can exist in extended devices. The modified preamble is usable for signaling, to legacy devices as well as extended devices, to indicate capabilities and to cause legacy devices or extended devices to defer to other devices such that the common communication channel is not subject to unnecessary interference. The modified preamble. is also usable for obtaining MIMO channel estimates and/or multi-channel estimates. The modified preamble preferably includes properties that facilitate detection of conventional and/or extended modes ("mode detection") and provides some level of coexistence with legacy IEEE 802.11a devices.

Claims	Prior Art
	Gardner '709 at FIG. 3  FIG. 3 Gardner '709 at [0014] FIG. 3 illustrates several devices coupled via a wireless network.
[1a] at least one receiver or transceiver for signal or data reception from one or more devices;	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “at least one receiver or transceiver for signal or data reception from one or more devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “at least one receiver or transceiver for signal or data reception from one or more devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “at least one receiver or transceiver for signal or data reception from one or more devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Engels '850 at Abstract An indoor to outdoor unit is described for placement outside of a building and adjacent to a structural part of the building. The unit has first antenna means (12) for communication with at least one indoor antenna

Claims	Prior Art
	(13) placed inside said building, the first antenna means having a reflector for reflecting radio signals towards the inside of the building. For instance, the first antenna means may be adapted to be located with respect to a wall of the building in such a way that a part of the wall is situated in the near-field region of the first antenna means. The first antenna means may be adapted for connection to a cable network. Alternatively; the unit may also have a second antenna means (10) for communication with at least one outdoor antenna (9) located outside the building. The first and second antenna means are adapted for attachment to or located in a housing. In operation some signals received by the second antenna means (10) from the one outdoor antenna (9) are transmitted to the first antenna means (12) and some signals transmitted from the second antenna means (10) to the one outdoor antenna (9) are received from the first antenna means (12) so that the unit acts as a repeater. Roesse '556 at Abstract A method for location discovery in a data network includes receiving, at a first device, connection information from a neighboring network device and determining a physical location of the first device based on the connection information. The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device be one of a variety of devices, such as a router, a switch, a network entry device, a firewall device, or a gateway.

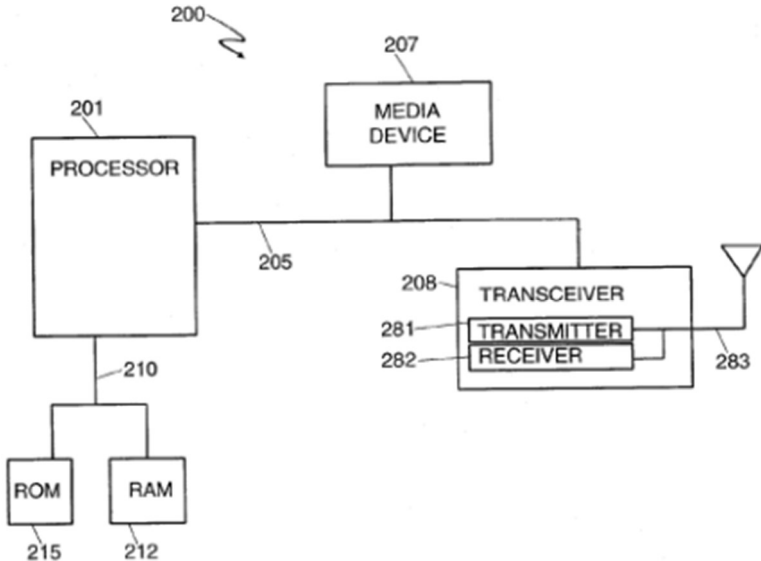
Claims	Prior Art																												
	Mbps and 480 Mbps over short ranges of less than 10 meters. The February 2002 FCC approval of ultra wideband (UWB) devices prompted many companies to consider UWB radio when proposing physical layers to IEEE 802.15.3a. Mandke 2003A at 5 TG3a has set out to develop a flexible standard which will enable high data rate WPAN (110 Mbps at 10m, 200 Mbps at 4m, and 480 Mbps at an unspecified distance) over a cost effective architecture. This new standard will enable a broad range of applications including the wireless transmission of images and video. The goal of this paper is to explore the unique design issues specific to UWB, engineering trade-offs faced by standards developers, and the current state of IEEE 802.15.3a. Section 2 will discuss the unique aspects of indoor UWB channels and the four of the proposed TG3a channel models. Section 3 compares a traditional impulse radio approach to UWB with a more recent multibanded approach (which has been employed in many TG3a proposals). Section 4 details the requirements and specifications set forth by IEEE 802.15.3a, and categorize the proposals being considered in order to form a clear picture of the current state of UWB technology as it relates to WPANs. Mandke 2003A at Page 24 <table border="1" data-bbox="638 849 1509 1344"> <thead> <tr> <th>Company</th><th>Texas Instruments</th></tr> </thead> <tbody> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>3 (additional bands can be added in the future)</td></tr> <tr> <td>Bandwidths</td><td>503.25 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.168 GHz – 4.752 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>TFI-OFDM, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>not available</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>312.5 ns OFDM symbol</td></tr> <tr> <td>Multipath mitigation method</td><td>1-tap (robust to 60.6 ns delay spread)</td></tr> </tbody> </table> A. Batra, et. al. "TI Physical Layer Proposal for IEEE 802.15 Task Group 3a," IEEE P802.15-03/142r0. March 3, 2003.	Company	Texas Instruments	Spectrum Allocation:		# of bands	3 (additional bands can be added in the future)	Bandwidths	503.25 MHz	Frequency ranges	3.168 GHz – 4.752 GHz	Modulation Scheme	TFI-OFDM, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	not available	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps	Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps	Symbol period	312.5 ns OFDM symbol	Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)
Company	Texas Instruments																												
Spectrum Allocation:																													
# of bands	3 (additional bands can be added in the future)																												
Bandwidths	503.25 MHz																												
Frequency ranges	3.168 GHz – 4.752 GHz																												
Modulation Scheme	TFI-OFDM, QPSK																												
Coexistence method	null band for WLAN (~5 GHz)																												
Multiple access method	not available																												
# of simultaneous piconets	not available																												
Error correction codes	Convolutional code																												
Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps																												
Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps																												
Symbol period	312.5 ns OFDM symbol																												
Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)																												

Claims	Prior Art																																																								
	Mandke 2003A at Page 24 <table border="1"> <tr> <th>Company</th><th>XtremeSpectrum</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>2</td></tr> <tr> <td>Bandwidths</td><td>1.368 GHz, 2.736 GHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>BPSK, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Ternary CDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>4 piconets/band</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Soloman code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps</td></tr> <tr> <td>Chip duration</td><td>731 ps (Low band), 365.5 ps (High band)</td></tr> <tr> <td>Multipath mitigation method</td><td>Decision feedback equalizer</td></tr> </table> R. Roberts, “XtremeSpectrum CFP Document,” IEEE P802.15-03/154r1. March 3, 2003. Mandke 2003A at Page 27 <table border="1"> <tr> <th>Company</th><th>Discrete Time</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>15 bands</td></tr> <tr> <td>Bandwidths</td><td>500 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 10.6 GHz,</td></tr> <tr> <td>Modulation Scheme</td><td>QPSK, FH</td></tr> <tr> <td>Coexistence method</td><td>sacrifice 2 band for WLAN coexistence (5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>FDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps</td></tr> <tr> <td>Link margin</td><td>15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps</td></tr> <tr> <td>Multipath mitigation method</td><td>not available</td></tr> </table> Roberto Aiello, “Discrete Time PHY Proposal for TG3a,” IEEE 802.15-03/099r1. March 2003.	Company	XtremeSpectrum	Spectrum Allocation:		# of bands	2	Bandwidths	1.368 GHz, 2.736 GHz	Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz	Modulation Scheme	BPSK, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	Ternary CDMA	# of simultaneous piconets	4 piconets/band	Error correction codes	Convolutional code, Reed-Soloman code	Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps	Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps	Chip duration	731 ps (Low band), 365.5 ps (High band)	Multipath mitigation method	Decision feedback equalizer	Company	Discrete Time	Spectrum Allocation:		# of bands	15 bands	Bandwidths	500 MHz	Frequency ranges	3.1 GHz – 10.6 GHz,	Modulation Scheme	QPSK, FH	Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)	Multiple access method	FDMA	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	½ @ 110 Mbps	Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps	Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps	Multipath mitigation method	not available
Company	XtremeSpectrum																																																								
Spectrum Allocation:																																																									
# of bands	2																																																								
Bandwidths	1.368 GHz, 2.736 GHz																																																								
Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz																																																								
Modulation Scheme	BPSK, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	Ternary CDMA																																																								
# of simultaneous piconets	4 piconets/band																																																								
Error correction codes	Convolutional code, Reed-Soloman code																																																								
Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps																																																								
Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps																																																								
Chip duration	731 ps (Low band), 365.5 ps (High band)																																																								
Multipath mitigation method	Decision feedback equalizer																																																								
Company	Discrete Time																																																								
Spectrum Allocation:																																																									
# of bands	15 bands																																																								
Bandwidths	500 MHz																																																								
Frequency ranges	3.1 GHz – 10.6 GHz,																																																								
Modulation Scheme	QPSK, FH																																																								
Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)																																																								
Multiple access method	FDMA																																																								
# of simultaneous piconets	not available																																																								
Error correction codes	Convolutional code																																																								
Code rates	½ @ 110 Mbps																																																								
Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps																																																								
Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps																																																								
Multipath mitigation method	not available																																																								

Claims	Prior Art
	Fontana at 2 UWB APPLICATIONS Figure 1 illustrates an ultra wideband, handheld transceiver that was designed for full duplex voice and data transmission at rates of up to 128 kb/s (CVSD) and 115.2 kb/s (RS232). The radio has an operational center frequency in L-band (1.5 GHz) with an instantaneous bandwidth of 400 MHz (27% fractional BW). Peak power output from the UWB transceiver was measured at 2.0 Watts, with a resultant average power (worst case) of 640 μW. This results in a worst case power density of 1.6 pW/Hz. These units have a range of approximately 1 to 2 km (with small antennas shown and line-of-sight), and an extended range of 10 to 20 miles with small gain antennas. Fontana at Figure 1  Figure 1. Full Duplex UWB Handheld Transceivers. Fontana at 3 Figure 3 illustrates a high-speed (up to 25 Mb/s) UWB radio designed for transmission of compressed video and command & control information across an asymmetric, bi-directional link. This system was also designed to operate in the 1.3 to 1.7 GHz region (27% fractional BW) with a 4W peak power output. An earlier design, developed under funding from the U.S. Defense Advanced research Projects Agency (DARPA), operated with a 500 MHz instantaneous bandwidth in the C-band region (5.4 to 5.9 GHz).

Claims	Prior Art
	Fontana at Figure 6 Figure 6. <i>UWB Wireless Intercom Communications System (WICS).</i> Fontana at 5 Ultra wideband technology was considered for this application because of its ability to transmit large amounts of data at high speed in a mobile, multipath-prone environment. The UWB tag operated in the L-band region (1.4 to 1.65 GHz) and had a peak output power of approximately 250 mW for a demonstrated range of over 300 meters. The image of the driver was stored as a compressed JPEG file, together with additional ASCII data, in EEPROM and periodically transmitted at a 400 kb/s burst rate to a UWB receiver with display. The tag operated off of two AAA batteries (3.0V) and, in an operational scenario, was mounted behind the front grill of the automobile. Fontana at 5 Figure 6 illustrates a set of prototype UWB transceivers designed for the U.S. Navy to provide a wireless intercom capability on-board Navy aircraft. The prototype UWB transceivers provide multichannel, full duplex, 32 kb/s digital voice over a range of approximately 100 meters. An ultra wideband waveform was selected because of its ability to operate in severe multipath (created by multiple RF reflections inside and around aircraft), and because of its non-interfering, low probability of intercept signature.

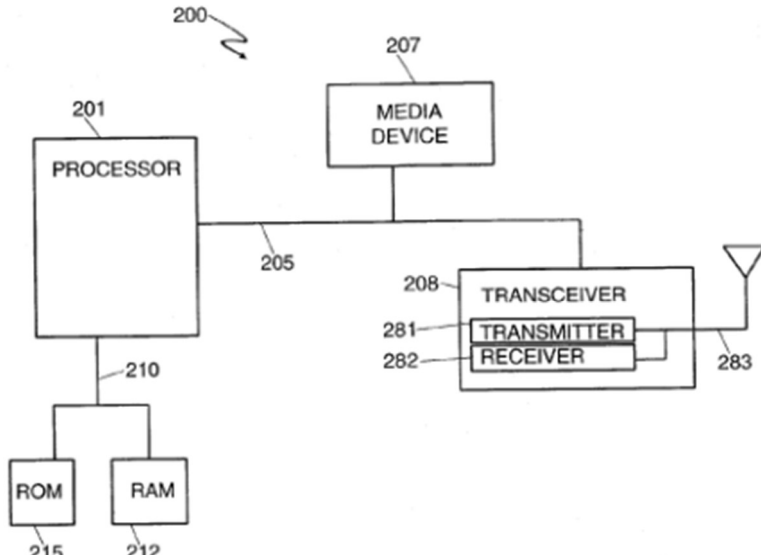
Claims	Prior Art
	Fontana at Figure 8 Figure 8. UWB Precision Geolocation System Transceiver. Fontana at 6 The system in Figure 8 utilizes a 2.5 ns, 4 Watt peak, UWB pulse, again operating in the 1.3 to 1.7 GHz region. Line-of-sight range for the system is better than 2 kilometers utilizing small, omnidirectional vertically polarized (smaller) or circularly polarized (larger) antennas. Within a building, the range becomes limited by wall and obstacle attenuation; however, ranges exceeding 100 meters inside have been attained. An unique feature of the system is the ability to detect the pulse leading edge through the use of a charge sensitive, tunnel diode detector. Leading edge detection is critical to the resolution of the direct path from the plethora of multipath returns produced from internal reflections. The UWB geolocation system was originally developed to permit a soldier to determine his or her position to within 1 foot resolution in an urban environment. It is currently being used to augment a video capture system for 3-D modeling, and for materiel location onboard a Navy ship. Fontana at Figure 10 Figure 10. UWB Backup Sensor. Fontana at 7 Several variants of the Hummingbird radar have also been developed. For example, Figure 10 illustrates an ultra wideband backup sensor for the detection of personnel, vehicles and other objects behind large construction and mining vehicles.

Claims	Prior Art
	[Figure 10] Operating with approximately 250 mW peak in the C-band region from 5.4 to 5.9 GHz, the backup sensor utilizes a dual antenna configuration for the detection of objects as close as 1 foot to beyond 350 feet from the vehicle. Ultra wideband provides a significant advantage for this application because of the ability to provide precision range gating to eliminate clutter which, with conventional Doppler-based sensors, often results in large false alarm rates. This sensor was developed for the National Institute of Occupational Safety and Health. Aiello '273 at Fig. 2  FIG. 2 Aiello '273 at [0045] Transceiver 208 receives and transmits data to processing unit 201 via I/O bus 205. Transceiver 208 includes a transmitter 281 which receives data from processing unit 201 and converts the data to UWB signals that are then applied to antenna 283 for transmission. In transmitter 208, circuitry may shape the time domain signal so that the associated spectrum optimizes the antenna transfer function for minimum transmission loss.

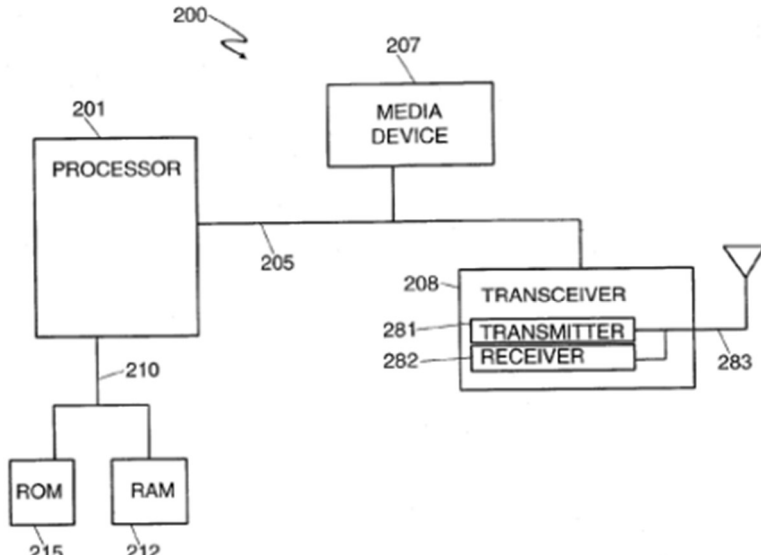
Claims	Prior Art
	Discrete Time Proposal at Slide 5 Summary • Compliant with FCC 02-48, UWB Report & Order • 3.1-10.6GHz, 500MHz band spacing • Varies symbol rate and number of bands, from 16Mbps to 600Mbps at PHY-SAP • Scalable down to lower bit rates for lower power, lower cost • Due to time constraints this presentation addresses – Frequency plan – Modulation scheme – Performance in AWGN channel – MAC considerations – Location awareness (contribution from Uri Kareev, Pulsicom) – Concepts of pulse shaping and multiple access • Remaining material will be presented at the next opportunity in May 2003 – Performance in multipath – Channelization – Implementation feasibility – Self evaluation criteria – Other issues that will emerge from group's feedback Chabas '657 at Abstract This telecommunications device (21, 22 or 23) forms part of a system comprising base stations (10, 12). This system permits the devices forming it to relay information among them. It is proposed to provide the devices with a plurality of transceiver devices (RX1, RX2, . . . , RXm, TX1, TX2, . . . , TXn) for exchanging information with other devices and/or base stations. Application: ODMA mobile radios Soomro '456 at [0008] To address the above-discussed deficiencies of the prior art, it is a primary object of the present invention to provide, for use in an independent basic service set (IBSS) network, a dynamic frequency selection (DFS) process enabled by a DFS element within beacon and probe response frames defining a DFS owner, a DFS interval specifying the time until channel switch in beacon intervals, a DFS count specifying a time in beacon intervals until the dynamic frequency selection owner initiates selection of the next operating channel frequency from the supported channel set, and a DFS recovery interval specifying a time after the end of the DFS interval when recovery procedures are initiated if no channel switch information was received during the past DFS interval. Channel switch information is presented in beacons following the end of the channel selection process, and within beacons during the DFS recovery

Claims	Prior Art
	interval. 802-15-3a at PAR Form, Page 2 The intent of this project is to provide a standard for a low complexity, low cost, low power consumption alternate PHY for 802.15.3 (comparable to the goals for 802.15.3). The data rate will be high enough, 110 Mb/s or more (see 18a), to satisfy an evolutionary set of consumer multi-media industry needs for WPAN communications. The project will address the requirements to support multimedia data types in multiple compliant co-located systems and also coexistence (18b). 14. Intellectual Property: Sponsor has reviewed the IEEE patent policy with the working group? Yes Sponsor is aware of copyrights relevant to this project? No Sponsor is aware of trademarks relevant to this project? No Sponsor is aware of possible registration of objects or numbers due to this project? No 15. Are you aware of other standards or projects with a similar scope? No Similar Scope Project Information: 16. Is there potential for this standard (in part or in whole) to be submitted to an international organization for review/adoption?: Do not Know If yes, please answer the following questions: Which International Organization/Committee? International Contact Information? 17. Will this project focus on Health, Safety or Environmental Issues? No 18. Additional Explanatory Notes: (Item Number and Explanation) 18a) The CFAs responses collected by study group 802.15 SG3a over the past several months indicate an evolutionary market developing for a group of applications that will not be addressed by 802.15.3. For example, high data rates, at least 110 Mb/s, will be required for simultaneous time dependent applications such as multiple HDTV video streams without sacrificing the requirements for low complexity, low cost, and low power consumption. In addition to at least 110 Mbps data rate, additional data rates, both lower and higher, may be supported. 18b) It is in the best interest of users and the industry to strive for a level of coexistence with other wireless systems, especially those in similar market spaces. Coexistence requirements will be established in SG3a selection criteria against which the proposals will be evaluated.
[1b] at least one transmitter or transceiver for signal or data transmission to one or more devices,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “at least one transmitter or transceiver for signal or data transmission to one or more devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “at least one transmitter or transceiver for signal or data transmission to one or more devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “at least one transmitter or transceiver for signal or data transmission to one or more devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. See above at row [1a].
[1c] wherein the transceiver for signal or data reception and the	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein the transceiver for signal or data reception and the transceiver for signal or data

Claims	Prior Art
transceiver for signal or data transmission may be the same or different; and	transmission may be the same or different.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Engels ’850 at Abstract An indoor to outdoor unit is described for placement outside of a building and adjacent to a structural part of the building. The unit has first antenna means (12) for communication with at least one indoor antenna (13) placed inside said building, the first antenna means having a reflector for reflecting radio signals towards the inside of the building. For instance, the first antenna means may be adapted to be located with respect to a wall of the building in such a way that a part of the wall is situated in the near-field region of the first antenna means. The first antenna means may be adapted for connection to a cable network. Alternatively; the unit may also have a second antenna means (10) for communication with at least one outdoor antenna (9) located outside the building. The first and second antenna means are adapted for attachment to or located in a housing. In operation some signals received by the second antenna means (10) from the one outdoor antenna (9) are transmitted to the first antenna means (12) and some signals transmitted from the second antenna means (10) to the one outdoor antenna (9) are received from the first antenna means (12) so that the unit acts as a repeater. Roose ’556 at Abstract A method for location discovery in a data network includes receiving, at a first device, connection information from a neighboring network device and determining a physical location of the first device based on the connection information. The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device be one of a variety of devices, such as a router, a switch, a network entry device, a firewall device, or a gateway.

Claims	Prior Art
	Aiello '273 at Fig. 2  FIG. 2 Aiello '273 at [0021] If the device has control of the system, the processor generates a control header including synchronization data. The synchronization data is used as described below by receiving devices to adjust a local clock for use in processing the received data. Encryption initialization data, link adaptation data, a source address of the transmitting device, a destination address of devices to receive the data, and a length of a data field of the packet may also be included in the control header. The control header is then placed in a data packet and sent to the transmitter. The transmitter then transmits the data packet using UWB. Aiello '273 at [0046] Receiver 282 receives UWB signals that are detected by antenna 283 and converts the UWB signals to data. The data is then transmitted to processing unit 201 over I/O bus 205. Receiver 282 is standard receiver for UWB signals and the particular design is omitted for brevity. One skilled in the art will recognize that that particular design of transceiver 208 and circuitry inside is left as design choice and transceiver 208 need only be configured to provide UWB transmission in accordance with this invention.

Claims	Prior Art
	Aiello '273 at [0055] fter the payload is generated, the processor in the transmitting device generates the payload in step 335 from the control header and generated payload. The processor then transmits the packet to the transceiver. The transmitter in the transceiver then transmits the packet in UWB signals. Chabas '657 at Abstract This telecommunications device (21, 22 or 23) forms part of a system comprising base stations (10, 12). This system permits the devices forming it to relay information among them. It is proposed to provide the devices with a plurality of transceiver devices (RX1, RX2, . . . , RXm, TX1, TX2, . . . , TXn) for exchanging information with other devices and/or base stations. Application: ODMA mobile radios
[1d] a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success.

Claims	Prior Art
	Aiello '273 at Fig. 2  FIG. 2 Aiello '273 at [0021] If the device has control of the system, the processor generates a control header including synchronization data. The synchronization data is used as described below by receiving devices to adjust a local clock for use in processing the received data. Encryption initialization data, link adaptation data, a source address of the transmitting device, a destination address of devices to receive the data, and a length of a data field of the packet may also be included in the control header. The control header is then placed in a data packet and sent to the transmitter. The transmitter then transmits the data packet using UWB. Aiello '273 at [0043] FIG. 2 illustrates a block diagram of a device 200 that operates as a device in decentralized system 100. Device 200 includes a processing unit 201. Processing unit 201 is a processor, microprocessor, controller or any combination thereof that executes instructions stored on a media to provide an application. Processor 201 is connected to a volatile memory such as Random Access Memory (RAM) 212 via memory bus 212. RAM 212 stores data and instructions which processing unit 201 uses to perform an application. Processor 201 is also connected to a non-volatile memory such Read Only Memory (ROM) 215 via memory bus 210. ROM 215 stores instructions for configuration and drivers needed by processing

Claims	Prior Art
	unit 201 to perform basic applications needed for set-up and control. Aiello '273 at [0044] Input/Output (I/O) Bus 205 connects processing unit 201 to media device 207 and transmitter 208. Media device 208 is a device that uses the data received via communications over a wireless network to provide a function. In a home entertainment system, media device 207 may be a television, a DVD player, speakers, a stereo or other such device. One skilled in the art will recognize that processing unit 201 may execute other application for providing other functions in media device 207 or may be a unit separate from the other functions of media device 207. Aiello '273 at [0059] A process 400 by which a device in decentralized network 100 receives and processes packets is illustrated in FIG. 4. Process 400 begins when a processor in a receiving device receives a packet that was converted to data by a receiver in the device from UWB signals received by the device in step 405. In step 410, the control header of the received packet is read. From the control header, the processor in receiving device determines whether the packet is addressed to the receiving device in step 420. If the packet is not addressed to the receiving device, process 400 may end or wait until another packet is received.
[1e] wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100 Megabits per second or more,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100 Megabits per second or more.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100 Megabits per second or more” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100

Claims	Prior Art
	Megabits per second or more” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Mandke 2003A at 2 IEEE 802.15.3 would not be able to provide the data rates necessary to support many of these applications. In November 2001, an additional task group within IEEE 802.15, Task Group 3a, was formed to identify a higher speed physical layer alternative that could support data rates between 110 Mbps and 480 Mbps over short ranges of less than 10 meters. The February 2002 FCC approval of ultra wideband (UWB) devices prompted many companies to consider UWB radio when proposing physical layers to IEEE 802.15.3a. Mandke 2003A at 3 In February of 2002, the FCC amended their Part 15 rules (concerning unlicensed radio devices) to include the operation of UWB devices without a license. The FCC defines UWB signals as having a fractional bandwidth of greater than 0.20 or a UWB bandwidth greater than 500 MHz. UWB bandwidth is defined as “the frequency band bounded by the points that are 10 dB below the highest radiated emission” [2]. Mandke 2003A at 5 TG3a has set out to develop a flexible standard which will enable high data rate WPAN (110 Mbps at 10m, 200 Mbps at 4m, and 480 Mbps at an unspecified distance) over a cost effective architecture. This new standard will enable a broad range of applications including the wireless transmission of images and video. The goal of this paper is to explore the unique design issues specific to UWB, engineering trade-offs faced by standards developers, and the current state of IEEE 802.15.3a. Section 2 will discuss the unique aspects of indoor UWB channels and the four of the proposed TG3a channel models. Section 3 compares a traditional impulse radio approach to UWB with a more recent multibanded approach (which has been employed in many TG3a proposals). Section 4 details the requirements and specifications set forth by IEEE 802.15.3a, and categorize the proposals being considered in order to form a clear picture of the current state of UWB technology as it relates to WPANs. Mandke 2003A at 12 Scalability parameters include; power consumption, payload bit rate and data throughput measured at the PHY-service access point (PHY-SAP), channelization (physical or coding), complexity, range, frequencies of operation, occupied bandwidth of operation, and other functions deemed appropriate. The

Claims	Prior Art																												
	alt-PHY should scale up to 480 Mbps and beyond, as well as 110Mbps and below. The MAC should be able to support the scaling of the alt-PHY. Mandke 2003A at 12 The proposed PHY should operate in the close proximity of multiple uncoordinated piconets, at bit rates of 110 Mbps, 200 Mbps and the optional 480 Mbps. A minimum of 200 packets should be used in estimating the packet error rate. Mandke 2003A at Table 4 <table border="1"> <tr> <th>Company</th><th>Texas Instruments</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>3 (additional bands can be added in the future)</td></tr> <tr> <td>Bandwidths</td><td>503.25 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.168 GHz – 4.752 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>TFI-OFDM, QPSK</td></tr> </table> 13 Mandke 2003A at Table 4 <table border="1"> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>not available</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>312.5 ns OFDM symbol</td></tr> <tr> <td>Multipath mitigation method</td><td>1-tap (robust to 60.6 ns delay spread)</td></tr> </table> Table 4: Overview of the TI Physical Layer Proposal for IEEE 802.15.3a [22].	Company	Texas Instruments	Spectrum Allocation:		# of bands	3 (additional bands can be added in the future)	Bandwidths	503.25 MHz	Frequency ranges	3.168 GHz – 4.752 GHz	Modulation Scheme	TFI-OFDM, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	not available	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps	Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps	Symbol period	312.5 ns OFDM symbol	Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)
Company	Texas Instruments																												
Spectrum Allocation:																													
# of bands	3 (additional bands can be added in the future)																												
Bandwidths	503.25 MHz																												
Frequency ranges	3.168 GHz – 4.752 GHz																												
Modulation Scheme	TFI-OFDM, QPSK																												
Coexistence method	null band for WLAN (~5 GHz)																												
Multiple access method	not available																												
# of simultaneous piconets	not available																												
Error correction codes	Convolutional code																												
Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps																												
Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps																												
Symbol period	312.5 ns OFDM symbol																												
Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)																												

Claims	Prior Art																																																								
	Mandke 2003A at Table 5 <table border="1"> <tr> <th>Company</th><th>XtremeSpectrum</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>2</td></tr> <tr> <td>Bandwidths</td><td>1.368 GHz, 2.736 GHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>BPSK, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Avoidance</td></tr> <tr> <td># of simultaneous piconets</td><td>Ternary CDMA</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Soloman code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps</td></tr> <tr> <td>Chip duration</td><td>731 ps (Low band), 365.5 ps (High band)</td></tr> <tr> <td>Multipath mitigation method</td><td>Decision feedback equalizer</td></tr> </table> Table 5: Overview of the XtremeSpectrum CFP Document [23]. Mandke 2003A at Table 6 <table border="1"> <tr> <th>Company</th><th>Intel</th></tr> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>7 (+ optional 6 bands for future use)</td></tr> <tr> <td>Bandwidths</td><td>550 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.6 GHz – 6.9 GHz, (7.45 GHz – 10.2 GHz optional)</td></tr> <tr> <td>Modulation Scheme</td><td>M-ary Bi-orthogonal Keying, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>DS/FH CDMA, optional FDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Soloman code</td></tr> <tr> <td>Code rates</td><td>6/32 @ 110 Mbps, 5/16 @ 200 Mbps, ¾ @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>6.3 dB @ 10 m @ 108 Mbps, 8.0 dB @ 4 m @ 288 Mbps, 4.0 dB @ 4 m @ 577 Mbps</td></tr> <tr> <td>Symbol period</td><td>3 ns</td></tr> <tr> <td>Multipath mitigation method</td><td>frequency interleaving of MBOK chips; time frequency codes; feed forward filter</td></tr> </table> Table 6: Overview of the Intel CFP Presentation for a UWB PHY [24].	Company	XtremeSpectrum	Spectrum Allocation:		# of bands	2	Bandwidths	1.368 GHz, 2.736 GHz	Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz	Modulation Scheme	BPSK, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	Avoidance	# of simultaneous piconets	Ternary CDMA	Error correction codes	Convolutional code, Reed-Soloman code	Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps	Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps	Chip duration	731 ps (Low band), 365.5 ps (High band)	Multipath mitigation method	Decision feedback equalizer	Company	Intel	Spectrum Allocation:		# of bands	7 (+ optional 6 bands for future use)	Bandwidths	550 MHz	Frequency ranges	3.6 GHz – 6.9 GHz, (7.45 GHz – 10.2 GHz optional)	Modulation Scheme	M-ary Bi-orthogonal Keying, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	DS/FH CDMA, optional FDMA	# of simultaneous piconets	not available	Error correction codes	Convolutional code, Reed-Soloman code	Code rates	6/32 @ 110 Mbps, 5/16 @ 200 Mbps, ¾ @ 480 Mbps	Link margin	6.3 dB @ 10 m @ 108 Mbps, 8.0 dB @ 4 m @ 288 Mbps, 4.0 dB @ 4 m @ 577 Mbps	Symbol period	3 ns	Multipath mitigation method	frequency interleaving of MBOK chips; time frequency codes; feed forward filter
Company	XtremeSpectrum																																																								
Spectrum Allocation:																																																									
# of bands	2																																																								
Bandwidths	1.368 GHz, 2.736 GHz																																																								
Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz																																																								
Modulation Scheme	BPSK, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	Avoidance																																																								
# of simultaneous piconets	Ternary CDMA																																																								
Error correction codes	Convolutional code, Reed-Soloman code																																																								
Code rates	½ @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps																																																								
Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps																																																								
Chip duration	731 ps (Low band), 365.5 ps (High band)																																																								
Multipath mitigation method	Decision feedback equalizer																																																								
Company	Intel																																																								
Spectrum Allocation:																																																									
# of bands	7 (+ optional 6 bands for future use)																																																								
Bandwidths	550 MHz																																																								
Frequency ranges	3.6 GHz – 6.9 GHz, (7.45 GHz – 10.2 GHz optional)																																																								
Modulation Scheme	M-ary Bi-orthogonal Keying, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	DS/FH CDMA, optional FDMA																																																								
# of simultaneous piconets	not available																																																								
Error correction codes	Convolutional code, Reed-Soloman code																																																								
Code rates	6/32 @ 110 Mbps, 5/16 @ 200 Mbps, ¾ @ 480 Mbps																																																								
Link margin	6.3 dB @ 10 m @ 108 Mbps, 8.0 dB @ 4 m @ 288 Mbps, 4.0 dB @ 4 m @ 577 Mbps																																																								
Symbol period	3 ns																																																								
Multipath mitigation method	frequency interleaving of MBOK chips; time frequency codes; feed forward filter																																																								

Claims	Prior Art																																																								
	Mandke 2003A at Page 24 <table border="1"> <thead> <tr> <th>Company</th><th>Texas Instruments</th></tr> </thead> <tbody> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>3 (additional bands can be added in the future)</td></tr> <tr> <td>Bandwidths</td><td>503.25 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.168 GHz – 4.752 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>TFI-OFDM, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>not available</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>312.5 ns OFDM symbol</td></tr> <tr> <td>Multipath mitigation method</td><td>1-tap (robust to 60.6 ns delay spread)</td></tr> </tbody> </table> A. Batra, et. al. "TI Physical Layer Proposal for IEEE 802.15 Task Group 3a," IEEE P802.15-03/142r0. March 3, 2003. Mandke 2003A at Page 24 <table border="1"> <thead> <tr> <th>Company</th><th>XtremeSpectrum</th></tr> </thead> <tbody> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>2</td></tr> <tr> <td>Bandwidths</td><td>1.368 GHz, 2.736 GHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz</td></tr> <tr> <td>Modulation Scheme</td><td>BPSK, QPSK</td></tr> <tr> <td>Coexistence method</td><td>null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Ternary CDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>4 piconets/band</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Soloman code</td></tr> <tr> <td>Code rates</td><td>1/2 @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps</td></tr> <tr> <td>Chip duration</td><td>731 ps (Low band), 365.5 ps (High band)</td></tr> <tr> <td>Multipath mitigation method</td><td>Decision feedback equalizer</td></tr> </tbody> </table> R. Roberts, "XtremeSpectrum CFP Document," IEEE P802.15-03/154r1. March 3, 2003.	Company	Texas Instruments	Spectrum Allocation:		# of bands	3 (additional bands can be added in the future)	Bandwidths	503.25 MHz	Frequency ranges	3.168 GHz – 4.752 GHz	Modulation Scheme	TFI-OFDM, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	not available	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps	Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps	Symbol period	312.5 ns OFDM symbol	Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)	Company	XtremeSpectrum	Spectrum Allocation:		# of bands	2	Bandwidths	1.368 GHz, 2.736 GHz	Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz	Modulation Scheme	BPSK, QPSK	Coexistence method	null band for WLAN (~5 GHz)	Multiple access method	Ternary CDMA	# of simultaneous piconets	4 piconets/band	Error correction codes	Convolutional code, Reed-Soloman code	Code rates	1/2 @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps	Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps	Chip duration	731 ps (Low band), 365.5 ps (High band)	Multipath mitigation method	Decision feedback equalizer
Company	Texas Instruments																																																								
Spectrum Allocation:																																																									
# of bands	3 (additional bands can be added in the future)																																																								
Bandwidths	503.25 MHz																																																								
Frequency ranges	3.168 GHz – 4.752 GHz																																																								
Modulation Scheme	TFI-OFDM, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	not available																																																								
# of simultaneous piconets	not available																																																								
Error correction codes	Convolutional code																																																								
Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps, 3/4 @ 480 Mbps																																																								
Link margin	5.5 dB @ 10 m @ 110 Mbps, 10.2 dB @ 4 m @ 200 Mbps, 12.2 dB @ 2 m @ 480 Mbps																																																								
Symbol period	312.5 ns OFDM symbol																																																								
Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)																																																								
Company	XtremeSpectrum																																																								
Spectrum Allocation:																																																									
# of bands	2																																																								
Bandwidths	1.368 GHz, 2.736 GHz																																																								
Frequency ranges	3.1 GHz – 5.15 GHz, 5.825 GHz – 10.6 GHz																																																								
Modulation Scheme	BPSK, QPSK																																																								
Coexistence method	null band for WLAN (~5 GHz)																																																								
Multiple access method	Ternary CDMA																																																								
# of simultaneous piconets	4 piconets/band																																																								
Error correction codes	Convolutional code, Reed-Soloman code																																																								
Code rates	1/2 @ 110 Mbps, RS(255,223) @ 200 Mbps, RS(255,223) @ 480 Mbps																																																								
Link margin	9.9 dB @ 10 m @ 110 Mbps, 13.2 dB @ 4 m @ 200 Mbps, 3.4 dB @ 2 m @ 600 Mbps																																																								
Chip duration	731 ps (Low band), 365.5 ps (High band)																																																								
Multipath mitigation method	Decision feedback equalizer																																																								

Claims	Prior Art																												
	Mandke 2003A at Page 27 <table border="1"> <thead> <tr> <th>Company</th><th>Discrete Time</th></tr> </thead> <tbody> <tr> <td colspan="2">Spectrum Allocation:</td></tr> <tr> <td># of bands</td><td>15 bands</td></tr> <tr> <td>Bandwidths</td><td>500 MHz</td></tr> <tr> <td>Frequency ranges</td><td>3.1 GHz – 10.6 GHz,</td></tr> <tr> <td>Modulation Scheme</td><td>QPSK, FH</td></tr> <tr> <td>Coexistence method</td><td>sacrifice 2 band for WLAN coexistence (5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>FDMA</td></tr> <tr> <td># of simultaneous piconets</td><td>not available</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>½ @ 110 Mbps</td></tr> <tr> <td>Link margin</td><td>15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps</td></tr> <tr> <td>Multipath mitigation method</td><td>not available</td></tr> </tbody> </table> Roberto Aiello, "Discrete Time PHY Proposal for TG3a," IEEE 802.15-03/099r1. March 2003. Fontana at 2 UWB APPLICATIONS Figure 1 illustrates an ultra wideband, handheld transceiver that was designed for full duplex voice and data transmission at rates of up to 128 kb/s (CVSD) and 115.2 kb/s (RS232). The radio has an operational center frequency in L-band (1.5 GHz) with an instantaneous bandwidth of 400 MHz (27% fractional BW). Peak power output from the UWB transceiver was measured at 2.0 Watts, with a resultant average power (worst case) of 640 μW. This results in a worst case power density of 1.6 pW/Hz. These units have a range of approximately 1 to 2 km (with small antennas shown and line-of-sight), and an extended range of 10 to 20 miles with small gain antennas. Fontana at 3 Figure 3 illustrates a high-speed (up to 25 Mb/s) UWB radio designed for transmission of compressed video and command & control information across an asymmetric, bi-directional link. This system was also designed to operate in the 1.3 to 1.7 GHz region (27% fractional BW) with a 4W peak power output. An earlier design, developed under funding from the U.S. Defense Advanced research Projects Agency (DARPA), operated with a 500 MHz instantaneous bandwidth in the C-band region (5.4 to 5.9 GHz).	Company	Discrete Time	Spectrum Allocation:		# of bands	15 bands	Bandwidths	500 MHz	Frequency ranges	3.1 GHz – 10.6 GHz,	Modulation Scheme	QPSK, FH	Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)	Multiple access method	FDMA	# of simultaneous piconets	not available	Error correction codes	Convolutional code	Code rates	½ @ 110 Mbps	Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps	Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps	Multipath mitigation method	not available
Company	Discrete Time																												
Spectrum Allocation:																													
# of bands	15 bands																												
Bandwidths	500 MHz																												
Frequency ranges	3.1 GHz – 10.6 GHz,																												
Modulation Scheme	QPSK, FH																												
Coexistence method	sacrifice 2 band for WLAN coexistence (5 GHz)																												
Multiple access method	FDMA																												
# of simultaneous piconets	not available																												
Error correction codes	Convolutional code																												
Code rates	½ @ 110 Mbps																												
Link margin	15.1 dB @ 4m @ 110 Mbps, 12 dB @ 4 m @ 220 Mbps, 11.1 dB @ 4 m @ 480 Mbps																												
Symbol period	8.9 ns @ 110 Mbps, 4.5 ns @ 200 Mbps, 2.1 ns @ 480 Mbps																												
Multipath mitigation method	not available																												

Claims	Prior Art
	Fontana at 5 Ultra wideband technology was considered for this application because of its ability to transmit large amounts of data at high speed in a mobile, multipath-prone environment. The UWB tag operated in the L-band region (1.4 to 1.65 GHz) and had a peak output power of approximately 250 mW for a demonstrated range of over 300 meters. The image of the driver was stored as a compressed JPEG file, together with additional ASCII data, in EEPROM and periodically transmitted at a 400 kb/s burst rate to a UWB receiver with display. The tag operated off of two AAA batteries (3.0V) and, in an operational scenario, was mounted behind the front grill of the automobile. Fontana at Figure 8 Figure 8. UWB Precision Geolocation System Transceiver. Fontana at 6 The system in Figure 8 utilizes a 2.5 ns, 4 Watt peak, UWB pulse, again operating in the 1.3 to 1.7 GHz region. Line-of-sight range for the system is better than 2 kilometers utilizing small, omnidirectional vertically polarized (smaller) or circularly polarized (larger) antennas. Within a building, the range becomes limited by wall and obstacle attenuation; however, ranges exceeding 100 meters inside have been attained. An unique feature of the system is the ability to detect the pulse leading edge through the use of a charge sensitive, tunnel diode detector. Leading edge detection is critical to the resolution of the direct path from the plethora of multipath returns produced from internal reflections. The UWB geolocation system was originally developed to permit a soldier to determine his or her position to within 1 foot resolution in an urban environment. It is currently being used to augment a video capture system for 3-D modeling, and for materiel location onboard a Navy ship.

Claims	Prior Art
	Fontana at Figure 10  Figure 10. UWB Backup Sensor. Fontana at 7 Several variants of the Hummingbird radar have also been developed. For example, Figure 10 illustrates an ultra wideband backup sensor for the detection of personnel, vehicles and other objects behind large construction and mining vehicles. [Figure 10] Operating with approximately 250 mW peak in the C-band region from 5.4 to 5.9 GHz, the backup sensor utilizes a dual antenna configuration for the detection of objects as close as 1 foot to beyond 350 feet from the vehicle. Ultra wideband provides a significant advantage for this application because of the ability to provide precision range gating to eliminate clutter which, with conventional Doppler-based sensors, often results in large false alarm rates. This sensor was developed for the National Institute of Occupational Safety and Health. Aiello '273 at [0003] The present invention relates to a system for transmitting data using Ultra Wide Band (UWB) radio frequencies. More particularly, this invention relates to a system using UWB to transmit data in a decentralized system and where the data is time sensitive. Still more particularly, this invention relates to transmitting data using UWB in a home entertainment system. Aiello '273 at [0014] UWB is a form of radio transmission. UWB employs short pulses of energy that spread across a wide range of frequencies. A UWB signal is a radio signal with a fractional bandwidth larger than 25%. For example, a UWB signal with a center frequency of 3 GHz has a minimum bandwidth of 750 MHz. Unlike conventional RF technologies, UWB modulates information into RF signals with a series of baseband, pulsed emissions transmitted without a carrier signal.

Claims	Prior Art
	Aiello '273 at [0015] Therefore UWB has several inherent features that make UWB desirable for use for wireless communications for systems, such as home entertainment systems. First, UWB signals utilize a spectrum of frequencies already designated for other devices. Secondly, UWB signals also have a low power density which allows coexistence with other RF devices with minimal interference. Thirdly, UWB has a low probability of multi-path fading and interference. Aiello '273 at [0017] The above and other problems are solved and an advance in the art is made by the De-centralized UWB system of this invention. This invention provides a wireless system that has a high data transfer rate required for multi-media applications such as video. This invention also provides high stability under a wide range of loads. Loads mean the amount of RF transmissions in an environment. This invention also provides a wireless system that supports mixed traffic. Mixed traffic is priority, dedicated traffic such as video and audio data as well as burst traffic used for applications such as Internet access. Aiello '273 at [0019] In accordance with this invention, each device in the system includes a transceiver having an RF transmitter and RF receiver. The transmitter and receiver are each configured to operate with UWB signals. The transceiver is connected to a processing unit that executes applications to transmit and receive data packets via UWB. Aiello '273 at [0020] The processing unit executes instructions from software stored in a memory of firmware to transmit data in accordance with this invention. In accordance with this invention, the processor in a device that requires a data transmission receives UWB signals being transmitted. When the device detects the system is idle of transmissions, the processor directs the transmitter to transmit arbitration pulses. The processor then waits to receive arbitration pulse signals from other devices requiring a data transmission. The processor then determines whether device has control of the system. Aiello '273 at [0021] If the device has control of the system, the processor generates a control header including synchronization data. The synchronization data is used as described below by receiving devices to adjust a local clock for use in processing the received data. Encryption initialization data, link adaptation data, a source address of

Claims	Prior Art
	the transmitting device, a destination address of devices to receive the data, and a length of a data field of the packet may also be included in the control header. The control header is then placed in a data packet and sent to the transmitter. The transmitter then transmits the data packet using UWB. Aiello '273 at [0055] fter the payload is generated, the processor in the transmitting device generates the payload in step 335 from the control header and generated payload. The processor then transmits the packet to the transceiver. The transmitter in the transceiver then transmits the packet in UWB signals. Aiello '273 at [0059] A process 400 by which a device in decentralized network 100 receives and processes packets is illustrated in FIG. 4. Process 400 begins when a processor in a receiving device receives a packet that was converted to data by a receiver in the device from UWB signals received by the device in step 405. In step 410, the control header of the received packet is read. From the control header, the processor in receiving device determines whether the packet is addressed to the receiving device in step 420. If the packet is not addressed to the receiving device, process 400 may end or wait until another packet is received. Mandke 2003B at 23 On February 14, 2002, the FCC amended the Part 15 rules which govern unlicensed radio devices to include the operation of ultra wideband (UWB) devices. The use of UWB under the FCC guidelines [1] offers tremendous capacity potential (several Gbps) over short ranges (less than 10 meters) at low radiated power (mean EIRP of -41.3 dBm/MHz). The FCC defines UWB signals as having a fractional bandwidth (the ratio of baseband bandwidth to RF carrier frequency) of greater than 0.20, or a UWB bandwidth greater than 500 MHz. UWB bandwidth is defined as “the frequency band bounded by the points that are 10 dB below the highest radiated emission” [9].

Claims	Prior Art
	Mandke 2003B at Figure 2 <pre> graph TD A[IEEE 802.15 WPAN] --> B[IEEE 802.15.1] A --> C[IEEE 802.15.2] A --> D[IEEE 802.15.3] A --> E[IEEE 802.15.4] D --> F[IEEE 802.15.3a] </pre> IEEE 802.15.1 • Based on Bluetooth standard • 732 kbps • Range: 10 meters • Spectrum: 2.4 GHz ISM band IEEE 802.15.2 • Develop coexistence model and mechanism • Collaborative and non-collaborative coexistence between WLAN and WPAN IEEE 802.15.3 • 10 – 55 Mbps • Range: 30 – 50 meters • Spectrum: 2.4 GHz ISM band IEEE 802.15.3a • “Very” high data rate WPAN • 110 – 480 Mbps • Range: less than 10 m • Spectrum: 3.1 – 10.6 GHz IEEE 802.15.4 • Low power • 20 – 250 kbps • Range: 10 – 75 meters • Spectrum: 2.4 GHz band, 915 MHz band, and 868 MHz Figure 2 . Organization of IEEE 802.15. Mandke 2003B at 23 The fact that the FCC specified that UWB be a minimum bandwidth of 500 MHz is important—while UWB can occupy several GHz of bandwidth using small pulses (as pioneered by Xtreme Spectrum and Time Domain [23], [30]), the 500 MHz bandwidth rule has provided the impetus for chip makers to consider channelization, or a multiband approach, in the UWB standardization activity, mainly as a hedge against foreign governments who may not authorize the full U.S. 3.1 to 10.6 GHz allocation. Mandke 2003B at 24 The remainder of this article focuses on the up-to-the minute standardization activities of IEEE 802.15.3a, concerned with very high data rate WPAN, where UWB is employed. IEEE 802.15 Task Group 3a was formed in late 2001 to identify a higher speed physical layer alternative to 802.15.3. The IEEE 802.15.3a task group is aimed at developing physical layer standards to support data rates between 110 Mbps and 480 Mbps over short ranges of less than 10 meters (i.e. alternatives to the original IEEE 802.15.3 physical layer). It should be noted that 802.15.3.a is only concerned with physical layer alternatives and uses the same MAC layer as IEEE 802.15.3, which is described in [8].

Claims	Prior Art																										
	Mandke 2003B at Table 2 <table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Data rates (measured at PHY-SAP)</td><td>110, 220, and (optional) 480 Mbps</td></tr> <tr> <td>Range</td><td>10 m, 4 m and below</td></tr> <tr> <td>Power consumption</td><td>100 mW and 250 mW</td></tr> <tr> <td>Power management modes</td><td>Capabilities such as power save, wake up etc.</td></tr> <tr> <td>Co-located piconets</td><td>4</td></tr> <tr> <td>Interference susceptibility</td><td>Robust to IEEE systems, PER <8% for a 1024 byte packet</td></tr> <tr> <td>Co-existence capability</td><td>Reduced interference to IEEE systems, interfering average power at least 6 dB below the minimum sensitivity level of non-802.15.3a device</td></tr> <tr> <td>Cost</td><td>Similar to Bluetooth</td></tr> <tr> <td>Location awareness</td><td>Location information to be propagated to a suitable management entity</td></tr> <tr> <td>Scalability</td><td>Backwards compatibility with 802.15, adaptable to various regulatory regions (such as the US, European countries or Japan)</td></tr> <tr> <td>Signal Acquisition</td><td><20 μs for acquisition from the beginning of the preamble to the beginning of the header</td></tr> <tr> <td>Antenna practicality</td><td>Size and form factor consistent with original device</td></tr> </tbody> </table> Table 2 - Summary of Technical Requirements and Selection Criteria for 802.15.3a. (19, 20). Mandke 2003B at 25 The flexible standard to be developed by TG3a will enable data rates of 110 - 480 Mbps (data rates necessary for wireless USB), WPAN over a cost effective architecture, and will operate on the IEEE 802.15.3 MAC layer which is already well defined [8]. The new TG3a standard will enable a broad range of applications, including multimedia requiring in excess of 100 Mbps, such as wireless video conferencing.	Parameter	Value	Data rates (measured at PHY-SAP)	110, 220, and (optional) 480 Mbps	Range	10 m, 4 m and below	Power consumption	100 mW and 250 mW	Power management modes	Capabilities such as power save, wake up etc.	Co-located piconets	4	Interference susceptibility	Robust to IEEE systems, PER <8% for a 1024 byte packet	Co-existence capability	Reduced interference to IEEE systems, interfering average power at least 6 dB below the minimum sensitivity level of non-802.15.3a device	Cost	Similar to Bluetooth	Location awareness	Location information to be propagated to a suitable management entity	Scalability	Backwards compatibility with 802.15, adaptable to various regulatory regions (such as the US, European countries or Japan)	Signal Acquisition	<20 μ s for acquisition from the beginning of the preamble to the beginning of the header	Antenna practicality	Size and form factor consistent with original device
Parameter	Value																										
Data rates (measured at PHY-SAP)	110, 220, and (optional) 480 Mbps																										
Range	10 m, 4 m and below																										
Power consumption	100 mW and 250 mW																										
Power management modes	Capabilities such as power save, wake up etc.																										
Co-located piconets	4																										
Interference susceptibility	Robust to IEEE systems, PER <8% for a 1024 byte packet																										
Co-existence capability	Reduced interference to IEEE systems, interfering average power at least 6 dB below the minimum sensitivity level of non-802.15.3a device																										
Cost	Similar to Bluetooth																										
Location awareness	Location information to be propagated to a suitable management entity																										
Scalability	Backwards compatibility with 802.15, adaptable to various regulatory regions (such as the US, European countries or Japan)																										
Signal Acquisition	<20 μ s for acquisition from the beginning of the preamble to the beginning of the header																										
Antenna practicality	Size and form factor consistent with original device																										

Claims	Prior Art																										
	Mandke 2003B at Table 3 <table border="1"> <thead> <tr> <th colspan="2">Spectrum Allocation</th></tr> </thead> <tbody> <tr> <td>No. of bands</td><td>3 (1st generation bands), 10 optional bands</td></tr> <tr> <td>Bandwidths</td><td>528 MHz</td></tr> <tr> <td>Frequency ranges</td><td>Group A: 3.168-4.752 GHz Group B: 4.752-6.072 GHz Group C: 6.072-8.184 GHz Group D: 8.184-10.296 GHz</td></tr> <tr> <td>Modulation scheme</td><td>TFT-OFDM (with 128-point FFT), QPSK</td></tr> <tr> <td>Cocexistence method</td><td>Null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Time-frequency interleaving</td></tr> <tr> <td>No. of simultaneous piconets</td><td>4</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code</td></tr> <tr> <td>Code rates</td><td>11/32 @ 110 Mbps, 5/8 @ 200 Mbps 3/4 @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>5.3 dB @ 10 m @ 110 Mbps 10.0 dB @ 4 m @ 200 Mbps 11.5 dB @ 2 m @ 480 Mbps</td></tr> <tr> <td>Symbol period</td><td>312.5 ns OFDM symbol</td></tr> <tr> <td>Multipath mitigation method</td><td>1-tap (robust to 60.6 ns delay spread)</td></tr> </tbody> </table> Table 3 - Overview of the TI Multiband-OFDM Physical Layer proposal supported by the newly-formed Multiband-OFDM Coalition (28, 43). Mandke 2003B at 25 After its July 2003 meeting, TG3a is now left with two primary contenders: (1) The Texas Instruments OFDM-based multiband approach which uses 528 MHz channels (three mandatory lower band channels and four optional upper band channels) supported by the Multiband-OFDM Coalition, and (2) the Xtreme Spectrum-Motorola dual-band Impulse Radio spread spectrum approach, where there is a high band (above the 5.2 - 5.8 GHz unlicensed band) and a low band (from 3.1 GHz to just below the 5.2 - 5.8 GHz unlicensed band), and which exploits all of the UWB spectrum allocation.	Spectrum Allocation		No. of bands	3 (1st generation bands), 10 optional bands	Bandwidths	528 MHz	Frequency ranges	Group A: 3.168-4.752 GHz Group B: 4.752-6.072 GHz Group C: 6.072-8.184 GHz Group D: 8.184-10.296 GHz	Modulation scheme	TFT-OFDM (with 128-point FFT), QPSK	Cocexistence method	Null band for WLAN (~5 GHz)	Multiple access method	Time-frequency interleaving	No. of simultaneous piconets	4	Error correction codes	Convolutional code	Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps 3/4 @ 480 Mbps	Link margin	5.3 dB @ 10 m @ 110 Mbps 10.0 dB @ 4 m @ 200 Mbps 11.5 dB @ 2 m @ 480 Mbps	Symbol period	312.5 ns OFDM symbol	Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)
Spectrum Allocation																											
No. of bands	3 (1st generation bands), 10 optional bands																										
Bandwidths	528 MHz																										
Frequency ranges	Group A: 3.168-4.752 GHz Group B: 4.752-6.072 GHz Group C: 6.072-8.184 GHz Group D: 8.184-10.296 GHz																										
Modulation scheme	TFT-OFDM (with 128-point FFT), QPSK																										
Cocexistence method	Null band for WLAN (~5 GHz)																										
Multiple access method	Time-frequency interleaving																										
No. of simultaneous piconets	4																										
Error correction codes	Convolutional code																										
Code rates	11/32 @ 110 Mbps, 5/8 @ 200 Mbps 3/4 @ 480 Mbps																										
Link margin	5.3 dB @ 10 m @ 110 Mbps 10.0 dB @ 4 m @ 200 Mbps 11.5 dB @ 2 m @ 480 Mbps																										
Symbol period	312.5 ns OFDM symbol																										
Multipath mitigation method	1-tap (robust to 60.6 ns delay spread)																										

Claims	Prior Art																										
	Mandke 2003B at Table 4 <table border="1"> <thead> <tr> <th colspan="2">Spectrum Allocation</th></tr> </thead> <tbody> <tr> <td>No. of bands</td><td>2</td></tr> <tr> <td>Bandwidths</td><td>1.368 GHz, 2.736 GHz</td></tr> <tr> <td>Frequency ranges</td><td>3.2 – 5.15 GHz 5.825 – 10.6 GHz</td></tr> <tr> <td>Modulation scheme</td><td>BPSK, QPSK, DS-SS</td></tr> <tr> <td>Coexistence method</td><td>Null band for WLAN (~5 GHz)</td></tr> <tr> <td>Multiple access method</td><td>Ternary CDMA</td></tr> <tr> <td>No. of simultaneous piconets</td><td>8</td></tr> <tr> <td>Error correction codes</td><td>Convolutional code, Reed-Solomon code</td></tr> <tr> <td>Code rates</td><td>1/2 @ 110 Mbps RS(255,223) @ 200 Mbps RS(255,223) @ 480 Mbps</td></tr> <tr> <td>Link margin</td><td>6.7 dB @ 10 m @ 114 Mbps 11.9 dB @ 4 m @ 200 Mbps 1.7 dB @ 2 m @ 600 Mbps</td></tr> <tr> <td>Chip time</td><td>731 ps (Low band), 365.5 ps (High band)</td></tr> <tr> <td>Multipath mitigation method</td><td>Decision feedback equalizer and RAKE</td></tr> </tbody> </table> Table 4 - Overview of the Xtreme Spectrum CFP Document (30). Discrete Time Proposal at Slide 4 • Meet all system requirements – 7.1dB link margin at 110Mbps (30ft) – 12dB link margin at 220Mbps (12ft) – 11.1dB link margin at 480Mbps (12ft)	Spectrum Allocation		No. of bands	2	Bandwidths	1.368 GHz, 2.736 GHz	Frequency ranges	3.2 – 5.15 GHz 5.825 – 10.6 GHz	Modulation scheme	BPSK, QPSK, DS-SS	Coexistence method	Null band for WLAN (~5 GHz)	Multiple access method	Ternary CDMA	No. of simultaneous piconets	8	Error correction codes	Convolutional code, Reed-Solomon code	Code rates	1/2 @ 110 Mbps RS(255,223) @ 200 Mbps RS(255,223) @ 480 Mbps	Link margin	6.7 dB @ 10 m @ 114 Mbps 11.9 dB @ 4 m @ 200 Mbps 1.7 dB @ 2 m @ 600 Mbps	Chip time	731 ps (Low band), 365.5 ps (High band)	Multipath mitigation method	Decision feedback equalizer and RAKE
Spectrum Allocation																											
No. of bands	2																										
Bandwidths	1.368 GHz, 2.736 GHz																										
Frequency ranges	3.2 – 5.15 GHz 5.825 – 10.6 GHz																										
Modulation scheme	BPSK, QPSK, DS-SS																										
Coexistence method	Null band for WLAN (~5 GHz)																										
Multiple access method	Ternary CDMA																										
No. of simultaneous piconets	8																										
Error correction codes	Convolutional code, Reed-Solomon code																										
Code rates	1/2 @ 110 Mbps RS(255,223) @ 200 Mbps RS(255,223) @ 480 Mbps																										
Link margin	6.7 dB @ 10 m @ 114 Mbps 11.9 dB @ 4 m @ 200 Mbps 1.7 dB @ 2 m @ 600 Mbps																										
Chip time	731 ps (Low band), 365.5 ps (High band)																										
Multipath mitigation method	Decision feedback equalizer and RAKE																										

Claims	Prior Art
	Discrete Time Proposal at Slide 5 <i>Summary</i> • Compliant with FCC 02-48, UWB Report & Order • 3.1-10.6GHz, 500MHz band spacing • Varies symbol rate and number of bands, from 16Mbps to 600Mbps at PHY-SAP • Scalable down to lower bit rates for lower power, lower cost • Due to time constraints this presentation addresses – Frequency plan – Modulation scheme – Performance in AWGN channel – MAC considerations – Location awareness (contribution from Uri Kareev, Pulsicom) – Concepts of pulse shaping and multiple access • Remaining material will be presented at the next opportunity in May 2003 – Performance in multipath – Channelization – Implementation feasibility – Self evaluation criteria – Other issues that will emerge from group's feedback

Claims	Prior Art
	Discrete Time Proposal at Slide 7 <i>FCC compliant</i> • It is UWB but is similar in principle to frequency hopping • FCC compliant according to FCC UWB R&O • In this proposal the transmit signal occupies 500MHz at all times: frequency change is used to reduce ISI, not to spread the spectrum • “Thus, as long as the transmission system complies with the fractional bandwidth or minimum bandwidth requirements at all times during its transmission, we agree that it should be permitted to operate under the UWB regulations. We recognize that this may preclude certain types of modulations, such as swept frequency (e.g., FMCW), stepped frequency or frequency hopping systems. The current measurement procedures require that measurements of swept frequency devices be made with the frequency sweep stopped.” [FCC UWB R&O, B-32]

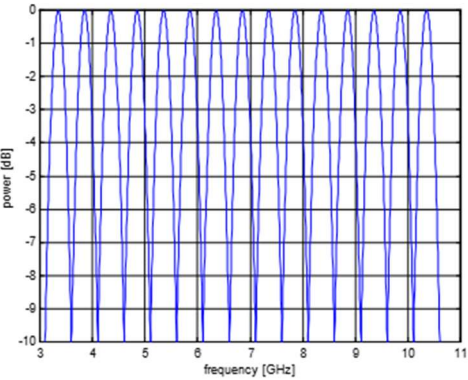
Claims

Prior Art

Discrete Time Proposal at Slide 8

Multi-band frequency plan

band#	fc (GHz)	f1 (GHz)	f2 (GHz)
1	3.35	3.1	3.6
2	3.85	3.6	4.1
3	4.35	4.1	4.6
4	4.85	4.6	5.1
5	5.35	5.1	5.6
6	5.85	5.6	6.1
7	6.35	6.1	6.6
8	6.85	6.6	7.1
9	7.35	7.1	7.6
10	7.85	7.6	8.1
11	8.35	8.1	8.6
12	8.85	8.6	9.1
13	9.35	9.1	9.6
14	9.85	9.6	10.1
15	10.35	10.1	10.6



- 500MHz bandwidth at -10dB point
- Spaced 500MHz away

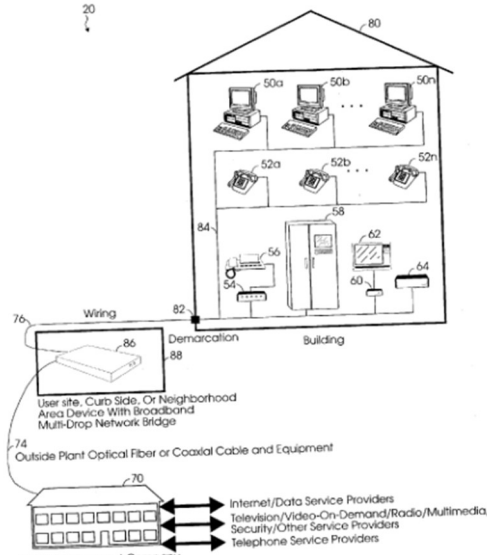
Claims	Prior Art																																																																
	Discrete Time Proposal at Slide 10 <i>Modes parameters (Mbps vs. bands and hopping frequency)</i> <table><tr><th># of bands/Hopping freq (MHz)</th><th>16</th><th>32</th><th>40</th></tr><tr><td>1</td><td>16</td><td>32</td><td>40</td></tr><tr><td>2</td><td>32</td><td>64</td><td>80</td></tr><tr><td>3</td><td>48</td><td>96</td><td>120</td></tr><tr><td>4</td><td>64</td><td>128</td><td>160</td></tr><tr><td>5</td><td>80</td><td>160</td><td>200</td></tr><tr><td>6</td><td>96</td><td>192</td><td>240</td></tr><tr><td>7</td><td>112</td><td>224</td><td>280</td></tr><tr><td>8</td><td>128</td><td>256</td><td>320</td></tr><tr><td>9</td><td>144</td><td>288</td><td>360</td></tr><tr><td>10</td><td>160</td><td>320</td><td>400</td></tr><tr><td>11</td><td>176</td><td>352</td><td>440</td></tr><tr><td>12</td><td>192</td><td>384</td><td>480</td></tr><tr><td>13</td><td>208</td><td>416</td><td>520</td></tr><tr><td>14</td><td>224</td><td>448</td><td>560</td></tr><tr><td>15</td><td>240</td><td>480</td><td>600</td></tr></table> Basic preamble rate Low bit rate mode Mandatory modes Optional mode	# of bands/Hopping freq (MHz)	16	32	40	1	16	32	40	2	32	64	80	3	48	96	120	4	64	128	160	5	80	160	200	6	96	192	240	7	112	224	280	8	128	256	320	9	144	288	360	10	160	320	400	11	176	352	440	12	192	384	480	13	208	416	520	14	224	448	560	15	240	480	600
# of bands/Hopping freq (MHz)	16	32	40																																																														
1	16	32	40																																																														
2	32	64	80																																																														
3	48	96	120																																																														
4	64	128	160																																																														
5	80	160	200																																																														
6	96	192	240																																																														
7	112	224	280																																																														
8	128	256	320																																																														
9	144	288	360																																																														
10	160	320	400																																																														
11	176	352	440																																																														
12	192	384	480																																																														
13	208	416	520																																																														
14	224	448	560																																																														
15	240	480	600																																																														

Claims	Prior Art																																																																																																																												
	Discrete Time Proposal at Slide 17 <i>Multiple access scheme: fractional bands</i> <table><tr><th>band#</th><th>fc (GHz)</th><th>fl (GHz)</th><th>fh (GHz)</th></tr><tr><td>1</td><td>3.35</td><td>3.1</td><td>3.6</td></tr><tr><td>2</td><td>3.85</td><td>3.6</td><td>4.1</td></tr><tr><td>3</td><td>4.35</td><td>4.1</td><td>4.6</td></tr><tr><td>4</td><td>4.85</td><td>4.6</td><td>5.1</td></tr><tr><td>5</td><td>5.35</td><td>5.1</td><td>5.6</td></tr><tr><td>6</td><td>5.85</td><td>5.6</td><td>6.1</td></tr><tr><td>7</td><td>6.35</td><td>6.1</td><td>6.6</td></tr><tr><td>8</td><td>6.85</td><td>6.6</td><td>7.1</td></tr><tr><td>9</td><td>7.35</td><td>7.1</td><td>7.6</td></tr><tr><td>10</td><td>7.85</td><td>7.6</td><td>8.1</td></tr><tr><td>11</td><td>8.35</td><td>8.1</td><td>8.6</td></tr><tr><td>12</td><td>8.85</td><td>8.6</td><td>9.1</td></tr><tr><td>13</td><td>9.35</td><td>9.1</td><td>9.6</td></tr><tr><td>14</td><td>9.85</td><td>9.6</td><td>10.1</td></tr><tr><td>15</td><td>10.35</td><td>10.1</td><td>10.6</td></tr></table><table><tr><th>band#</th><th>fc (GHz)</th><th>fl (GHz)</th><th>fh (GHz)</th></tr><tr><td>1.5</td><td>3.6</td><td>3.35</td><td>3.85</td></tr><tr><td>2.5</td><td>4.1</td><td>3.85</td><td>4.35</td></tr><tr><td>3.5</td><td>4.6</td><td>4.35</td><td>4.85</td></tr><tr><td>4.5</td><td>5.1</td><td>4.85</td><td>5.35</td></tr><tr><td>5.5</td><td>5.6</td><td>5.35</td><td>5.85</td></tr><tr><td>6.5</td><td>6.1</td><td>5.85</td><td>6.35</td></tr><tr><td>7.5</td><td>6.6</td><td>6.35</td><td>6.85</td></tr><tr><td>8.5</td><td>7.1</td><td>6.85</td><td>7.35</td></tr><tr><td>9.5</td><td>7.6</td><td>7.35</td><td>7.85</td></tr><tr><td>10.5</td><td>8.1</td><td>7.85</td><td>8.35</td></tr><tr><td>11.5</td><td>8.6</td><td>8.35</td><td>8.85</td></tr><tr><td>12.5</td><td>9.1</td><td>8.85</td><td>9.35</td></tr><tr><td>13.5</td><td>9.6</td><td>9.35</td><td>9.85</td></tr><tr><td>14.5</td><td>10.1</td><td>9.85</td><td>10.35</td></tr></table> • Fractional bands are placed between the integer bands: their center frequencies are 250MHz off with respect to the integer bands • This allows frequency division multiplexing • Collision with co-located piconets is further reduced by hopping sequences and low duty cycle	band#	fc (GHz)	fl (GHz)	fh (GHz)	1	3.35	3.1	3.6	2	3.85	3.6	4.1	3	4.35	4.1	4.6	4	4.85	4.6	5.1	5	5.35	5.1	5.6	6	5.85	5.6	6.1	7	6.35	6.1	6.6	8	6.85	6.6	7.1	9	7.35	7.1	7.6	10	7.85	7.6	8.1	11	8.35	8.1	8.6	12	8.85	8.6	9.1	13	9.35	9.1	9.6	14	9.85	9.6	10.1	15	10.35	10.1	10.6	band#	fc (GHz)	fl (GHz)	fh (GHz)	1.5	3.6	3.35	3.85	2.5	4.1	3.85	4.35	3.5	4.6	4.35	4.85	4.5	5.1	4.85	5.35	5.5	5.6	5.35	5.85	6.5	6.1	5.85	6.35	7.5	6.6	6.35	6.85	8.5	7.1	6.85	7.35	9.5	7.6	7.35	7.85	10.5	8.1	7.85	8.35	11.5	8.6	8.35	8.85	12.5	9.1	8.85	9.35	13.5	9.6	9.35	9.85	14.5	10.1	9.85	10.35
band#	fc (GHz)	fl (GHz)	fh (GHz)																																																																																																																										
1	3.35	3.1	3.6																																																																																																																										
2	3.85	3.6	4.1																																																																																																																										
3	4.35	4.1	4.6																																																																																																																										
4	4.85	4.6	5.1																																																																																																																										
5	5.35	5.1	5.6																																																																																																																										
6	5.85	5.6	6.1																																																																																																																										
7	6.35	6.1	6.6																																																																																																																										
8	6.85	6.6	7.1																																																																																																																										
9	7.35	7.1	7.6																																																																																																																										
10	7.85	7.6	8.1																																																																																																																										
11	8.35	8.1	8.6																																																																																																																										
12	8.85	8.6	9.1																																																																																																																										
13	9.35	9.1	9.6																																																																																																																										
14	9.85	9.6	10.1																																																																																																																										
15	10.35	10.1	10.6																																																																																																																										
band#	fc (GHz)	fl (GHz)	fh (GHz)																																																																																																																										
1.5	3.6	3.35	3.85																																																																																																																										
2.5	4.1	3.85	4.35																																																																																																																										
3.5	4.6	4.35	4.85																																																																																																																										
4.5	5.1	4.85	5.35																																																																																																																										
5.5	5.6	5.35	5.85																																																																																																																										
6.5	6.1	5.85	6.35																																																																																																																										
7.5	6.6	6.35	6.85																																																																																																																										
8.5	7.1	6.85	7.35																																																																																																																										
9.5	7.6	7.35	7.85																																																																																																																										
10.5	8.1	7.85	8.35																																																																																																																										
11.5	8.6	8.35	8.85																																																																																																																										
12.5	9.1	8.85	9.35																																																																																																																										
13.5	9.6	9.35	9.85																																																																																																																										
14.5	10.1	9.85	10.35																																																																																																																										

Claims	Prior Art
	Discrete Time Proposal at Slide 28 <i>Flexibility</i> • Scalable bit rate (from 16Mbps to 600Mbps) • Control individual bands to manage – Interference – Co-existence – Worldwide regulations • Scale power consumption – Variable number of bands – Variable hopping and symbol rate

Claims	Prior Art
	Discrete Time Proposal at Slide 29 Conclusions • UWB multi-band system • Similar to frequency hopping • Meet all system requirements – 7.1dB link margin at 110Mbps (30ft) – 12dB link margin at 220Mbps (12ft) – 11.1dB link margin at 480Mbps (12ft) • Low signal repetition frequency to reduce ISI and need for high speed digital circuits (lower power consumption) • “Narrow” UWB bandwidth to reduce complexity • Remaining material will be presented at the next opportunity in May 2003

Claims	Prior Art
	802-15-3a at PAR Form, Page 2 The intent of this project is to provide a standard for a low complexity, low cost, low power consumption alternate PHY for 802.15.3 (comparable to the goals for 802.15.3). The data rate will be high enough, 110 Mb/s or more (see 13a), to satisfy an evolutionary set of consumer multi-media industry needs for WPAN communications. The project will address the requirements to support multimedia data types in multiple compliant co-located systems and also coexistence (13b). 14. Intellectual Property: Sponsor has reviewed the IEEE patent policy with the working group? Yes Sponsor is aware of copyrights relevant to this project? No Sponsor is aware of trademarks relevant to this project? No Sponsor is aware of possible registration of objects or numbers due to this project? No 15. Are you aware of other standards or projects with a similar scope? No Similar Scope Project Information: 16. Is there potential for this standard (in part or in whole) to be submitted to an international organization for review/adoption?: Do not Know If yes, please answer the following questions: Which International Organization/Committee? International Contact Information? 17. Will this project focus on Health, Safety or Environmental Issues? No 18. Additional Explanatory Notes: (Item Number and Explanation) 18a) The CFAs responses collected by study group 802.15 SG3a over the past several months indicate an evolutionary market developing for a group of applications that will not be addressed by 802.15.3. For example, high data rates, at least 110 Mb/s, will be required for simultaneous time dependent applications such as multiple HDTV video streams without sacrificing the requirements for low complexity, low cost, and low power consumption. In addition to at least 110 Mbps data rate, additional data rates, both lower and higher, may be supported. 13b) It is in the best interest of users and the industry to strive for a level of coexistence with other wireless systems, especially those in similar market spaces. Coexistence requirements will be established in SG3a selection criteria against which the proposals will be evaluated.
[1f] wherein said broadband wireless repeater or relay is connected or connectable to one or more network backbones for connecting said one or more wireless networks with said one or more network backbones,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is connected or connectable to one or more network backbones for connecting said one or more wireless networks with said one or more network backbones.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is connected or connectable to one or more network backbones for connecting said one or more wireless networks with said one or more network backbones” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said broadband wireless repeater or relay is connected or connectable to one or more network backbones for connecting said one or more wireless networks with said one or more network backbones” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success.

Claims	Prior Art
	Bareis '373 at FIG. 2  FIG. 2 Bareis '373 at [0036] Referring now to FIG. 1, there is illustrated a first embodiment of a broadband multidrop local network 10 consistent with the present disclosure. Typically, network 10 may include a twisted-pair wire bus as exists in the outside plant 72 of a local interconnect company 70, such as a telephone company local exchange carrier (LEC), cable company office, or the like. Alternatively, the outside plant media could consist of coaxial cable in a cable network. It is also conceivable that optical versions of the embodiments of the present disclosure could be deployed using optical fiber to transport the data in the network. Bareis '373 at [0042] Referring now to FIG. 2, there is illustrated an alternate embodiment of the present disclosure directed to a very high speed data throughput. Very high speed data throughput has greater applicability in video-on-demand and video distribution applications, very fast Internet access, video telephony, and the like. In FIG. 2, a building 80 contains at least one network device to be connected via twisted-pair wire 84 to Local Interconnect Company 70 through demarcation point 82, thence via a short run of outside plant wiring 76, through a broadband multidrop local network interface 86, and finally through an outside plant optical fiber or coaxial cable 74. Devices that may be used on the network 20 must be compatible with the

Claims	Prior Art
	network interface 400 as will be described hereinbelow in conjunction with FIGS. 4 and 5. Such network devices may include, but are not limited to, computer systems 50 (a) . . . (n), telephone sets 52 (a) . . . (n), digital set top equipment 60, loop-start interface equipment 54, network-ready appliances 58, and security systems 64. Although not shown, other network devices such as television sets, high fidelity audio equipment, DVD or VCR devices, security cameras, utility metering equipment, facsimile machines, etc. each having a built-in network interface 400 may also be connected to the network 20. As described hereinabove, the local interconnect company 70 distributes packetized IP traffic between various service providers and the user site. Bareis '373 at [0058] In the configuration of FIG. 4, IP-based telephone set 52 is used to place and receive Voice over Internet Protocol (VoIP) calls through a service provider via optical fiber 74, broadband multidrop local network interface 86, and the copper wiring 72 and 84 interconnected at Demarcation 82. Bareis '373 at [0097] To summarize, there has been disclosed a broadband multidrop local network architecture for use in intercoupling multimedia traffic to and from a wide variety of addressable network devices. Each network device may be coupled via a network interface or broadband transceiver to a single wireline coupled to an external broadband communication service. Such communication service may be provided, e.g., via fiber optic link to a curbside terminal by an interconnection company, without requiring a complete secondary network and the associated equipment such as modems, routers, converters, hubs, switches, etc. The full data traffic capability at the full bandwidth achievable with relatively short runs (e.g., on the order of 100 meters) of twisted pair copper wire may be utilized when all traffic for all of the participating network devices is packetized on a wired medium for distribution thereon without the bandwidth, point-to-point, or data rate restrictions associated with conventional individual DSL (digital subscriber line) or similar services. In effect, the useable spectrum that exists on the broadband multidrop local network as disclosed hereinabove is a closed spectrum; that is, the entire bandwidth technically feasible on a twisted-pair medium over these relatively short distances is dedicated to the broadband communication capability implemented in each local network such that total data rates, with present standards and technologies, of at least 100 Mbps, and beyond to over 500 Mbps at reasonable distances, are available for each local network transferring data packets at the maximum packet rate of all network devices attachable thereto even when all of the network devices are transmitting. Each network device (computers, peripherals, telecommunications equipment, security systems, broadcast audio and video, to name just a few) may be assigned a bandwidth or packet data rate rating such that its use on the network appropriates a required

Claims	Prior Art
	portion of the total available data traffic capabilities of the network when in use and the user knows immediately what portion of his/her network capacity is being utilized. Roose '556 at 1:38–47 Computing systems are useful tools for the exchange of information among individuals. The information may include, but is not limited to, data, voice, graphics, and video. The exchange is established through interconnections linking the computing systems together in a way that permits the transfer of electronic signals that represent the information. The interconnections may be either cable or wireless. Cable connections include, for example, metal and optical fiber elements. Wireless connections include, for example infrared, acoustic, and radio wave transmissions.
[1g] wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices, and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Roose '556 at Abstract A method for location discovery in a data network includes receiving, at a first device, connection information from a neighboring network device and determining a physical location of the first device based on the connection information. The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device be one of a variety of devices, such as a router, a switch, a network entry device, a firewall device, or a gateway.

Claims	Prior Art
	Roose '556 at FIG> 4 501 <pre> graph TD 405[step 405: AUTHENTICATE USER ACCESS TO NETWORK BASED ON USER INFORMATION] --> 410[step 410: RECEIVE QUERY FROM USER SEEKING ACCESS TO NETWORK DATA, APPLICATION, RATE, SERVICE, RATE TYPE, ETC.] 410 --> 415[step 415: IDENTIFY LOCATION OF DEVICE ASSOCIATED WITH QUERYING USER] 415 --> 420[step 420: AUTHENTICATE LOCATION INFORMATION] 420 --> 425[step 425: IS USER AUTHENTICATED TO ACCESS REQUESTED INFORMATION APPLICATION?] 415 --> 425 425 -- N --> 440[step 440: DENY ACCESS NOTIFY NETWORK MANAGER NOTIFY USER] 425 -- Y --> 430[step 430: IS USER DEVICE LOCATED WHERE REQUESTED MATERIAL MAY BE SENT?] 430 -- N --> 440 430 -- Y --> 435[step 435: EXCHANGE DATA/ APPLICATION REQUESTED OR PROVIDE REQUESTED RULES] </pre> FIG. 4

Claims

Prior Art

Roose '556 at FIG. 5

500

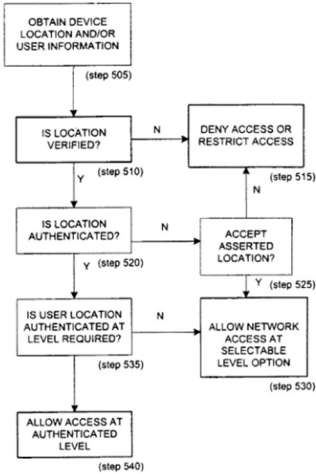
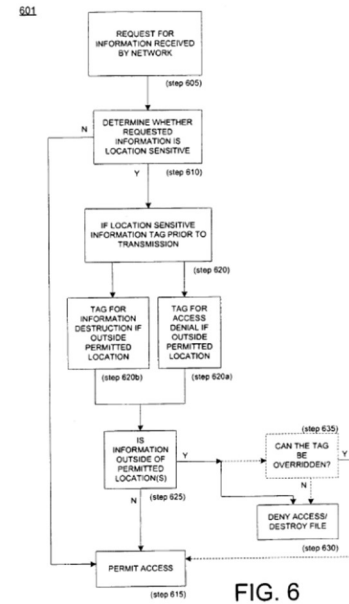


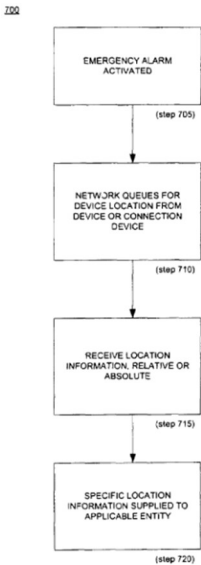
FIG. 5

Claims

Prior Art

Roose '556 at FIG. 6



Claims	Prior Art
	Roose '556 at FIG. 7  <pre> graph TD 705[EMERGENCY ALARM ACTIVATED] -- (step 705) --> 710[NETWORK QUEUES FOR DEVICE LOCATION FROM DEVICE OR CONNECTION DEVICE] 710 -- (step 710) --> 715[RECEIVE LOCATION INFORMATION, RELATIVE OR ABSOLUTE] 715 -- (step 715) --> 720[SPECIFIC LOCATION INFORMATION SUPPLIED TO APPLICABLE ENTITY] </pre> FIG. 7

Claims	Prior Art
	the device location can be used in any number of ways to enhance the operation of, and services provided by, the system. For example, anywhere user credentials are required, the location of a device can be required. In other words, the location of a device becomes part of the required credentials. Roese '556 at 2:66–3:12 The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The physical location can be a first physical location and the neighboring network device can be a first neighboring network device. In this example, the method can further include receiving, at the first device, a second physical location transmitted from a second neighboring network device and comparing the first physical location with the second physical location to determine a level of confidence of an actual physical location of the first device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device can include a router, a switch, a network entry device, a firewall device, or a gateway. Roese '556 at 3:14–38 In another aspect, there is a system including a location module. The location module is configured to determine a physical location of a connection point and to transmit the physical location to a client device in communication with the connection point. The system can further include the client device, configured to receive the physical location from the physical location module, and a neighboring network device in communication with the client device, the neighboring network device including the physical location module. The physical location can be a first physical location and the neighboring network device can be a first neighboring network device. In this example, the system can further include a second neighboring network device with a physical location module configured to determine a second physical location of the client device and transmit the second physical location to the client device. Further, the client device is further configured to receive the second physical location and to compare the first physical location with the second physical location to determine a level of confidence of an actual physical location of the client device. The system can associate a level of trust, based on the neighboring network device, with the physical location. The client device can include a router, a switch, a network entry device, a firewall device, a gateway, a wireless access point, and/or a computing device. Roese '556 at 4:5–29 Referring to FIG. 1, a location-aware system 100 operates and provides network-based services to users according to locations of devices that use or are part of the network associated with system 100. System 100 includes an infrastructure 101 that includes multiple switching devices, some of which are connected

Claims	Prior Art
	to connection points (e.g., 160a-i) of infrastructure 101. System 100 employs both hardware and software (e.g., an application executing on server 134) to provide location-aware services described below. A location of a device can relate to the physical location of the device, which can be characterized in a variety of ways including as grid or map coordinates (e.g., latitude, longitude, and elevation), a geographic region, or in terms of building structures, such as coordinates on a particular floor in a building or a room number in a building. A device can be external to infrastructure 101 of system 100, such as user devices 104a and 104b. A device also can be internal to infrastructure 101, such as network entry devices 114a-b (sometimes referred to as switches or edge devices of the network), and a central switching device 136 (e.g. a router). The network entry devices 114 can include and/or be associated with wireless access points 120a-b. The wireless access points 120 can be individual devices external to the network entry device 114, such as 120a and/or internal to the entry device 114, such as 120b. Roose '556 at 4:30–47 Some of the devices internal and external to infrastructure 101 include a location module 185. The location module 185 includes functionality, as described in more detail below, that makes a device location-aware. In one example, this functionality includes a location database to store location information, protocol to communicate location information to other devices, and rules to enforce location-based policies (e.g., to enable policing based on location information). This functionality can also include the algorithms and processes necessary to determine the location of a device using the techniques described herein. Location module 185 can be implemented in the hardware and/or software of system 100. For example, particular software applications executing on the devices can provide/enforce the location functions, the operating system of any of the devices can provide/enforce the location functions, and/or hardware modules, such as programmable arrays, can be used in the devices to provide/enforce the location functions. Roose '556 at 4:48–5:13 To make use of a device's location, system 100 first determines the location of that device. System 100 uses different techniques to determine the location of a device depending on whether the device communicates with other devices using a cable-based transmission medium 112, or a wireless transmission medium 119. Cable-based transmission medium 112 refers to a constrained transmission medium such as an optical cable, an electrical wire, and the like. Such a cable transmission medium can provide single to many connections (shared) and/or a point-to-point (dedicated) connection between two devices. A cable-based medium 112 can be considered as part of infrastructure 101 of system 100. Typically the medium 112 is installed in such a way that it is not easy to modify the medium's physical

Claims	Prior Art
	location. For instance, cables are lead through walls and conduits in such a way that the connection points (e.g., the jacks) are in fixed locations. Wireless transmission medium 119 refers to a transmission medium in a free space, such as though free air. Wireless transmission medium 119 generally relates to any communication where the transmission medium is air, for example, radio-based communication. For instance, radio communication according to the IEEE 802.11 standard uses a wireless transmission medium 119. Other wireless communication using wireless transmission media relate to use of optical communication (e.g., infra red, lasers, and the like) and/or other communications through air such as acoustic and mechanical waves. Wireless media are characterized by a much greater range of possible locations in which communicating devices may be located. For example, in the case of an IEEE 802.11 based network, a mobile device may be able to communicate with a wireless access point 120 hundreds or even thousands of feet away depending on the environment. Roose '556 at 8:28–44 Referring now to some detailed techniques for wireless connections, as described above, two example types of wireless communication chosen to illustrate these techniques are via radio frequencies or infrared frequencies. System 100 can employ different mechanisms for each of these types of communication. System 100 can employ a first group of mechanisms/techniques for identifying the location of a device (e.g., 104, 114) that communicates via radio frequencies. For example, system 100 triangulates the location of a device using one or more wireless access points, such as 120a-b, associated with network entry devices 114, such as 114a and 114b, respectively, as shown in FIG. 1. As another example, system 100 determines a device's location based on the proximity to an entry device. Following below is a listing of various techniques system 100 can employ to determine the location of a wireless device. Roose '556 at 8:45–61 System 100 can employ a number of known triangulation techniques, including the use of signal strength, angle of arrival, and relative time delay approaches. System 100 can employ off-frequency searching, such as by frequency hopping for short periods of time to detect stations on frequencies alternate to that employed for data exchange. For example, wireless access point 120a can operate at a first frequency f1. Wireless access point 120b can operate at a second frequency f2. Periodically, and for a relatively short period of time, wireless access point 120a operates at the second frequency f2 to detect and determine signal characteristics of a device communicating with wireless access point 120b. Similarly, wireless access point 120b periodically and for a relatively short period of time operates at the first frequency f1 to detect and determine signal characteristics of a device communicating with wireless access point 120a.

Claims	Prior Art
	Roese '556 at 8:62–9:6 System 100 can employ phased-array searches for lobe-based triangulation. That is, a radio antenna of the network entry device is directed to maximize or at least optimize lobe location as a search beacon. Such lobeing or lobe steering may be a staged process in which network entry devices 114 make broad sweeps to get rough location information, which may be sufficient in some situations. Network entry devices 114 can fine-tune the sweeps, if desired, with narrower lobes, to get a more accurate location. System 100 also can conduct phased-array antenna searches at off-frequency conditions (e.g., frequency hopping combined with directional searching). Roese '556 at 9:7–26 System 100 can perform calculations to approximate distance from a known access point (e.g., 120a-b) as a function of signal strength attenuation (e.g., the signal is at x strength so the device must be located in a range of y-z feet away). In addition to calculations, system 100 can also search stored associations of signal characteristics and their corresponding locations. This information can be stored in a signal characteristic database. A network administrator generates this signal characteristic database by measuring predefined signal characteristics at different locations and storing the measured characteristics for each of the locations. When subsequently determining a location of a user device, if system 100 detects a signal characteristic identically corresponding to a location, system 100 determines that the user device is at that corresponding location. If the signal characteristic is not identical, system 100 can use multiple entries within the database to extrapolate the user device location information based on the stored signal characteristic and location associations. This technique is sometimes referred to as RF training. Roese '556 at 9:27–46 Using multiple frequencies and/or connection-points and/or antennas may improve the accuracy of location derivation techniques. For example, if the same access point is used at different frequencies, system 100 can use the error in location information among the different frequencies to infer location more accurately. In addition, the use of multiple access points (e.g., signals from user device 104b received at 120a compared with signals received at 120b) may improve relative location accuracy in a type of triangulation or averaging of signal strength indicators. System 100 can employ multiple antennas for that purpose. Multiple antennas (not shown) may also be used to assert a line of bearing. In that case, the relative separation of the antennas and the accuracy of the known spacing both may provide improved location accuracy. System 100 also can employ ultra wide band waves to determine relative location of one or more devices. As the accuracy of the location derivation increases by using these improved techniques, system 100 can assign a higher value for the level of trust parameter associated with that

Claims	Prior Art
	location. Roose '556 at 9:47–10:2 System 100 also can use signal amplitude differential from the network entry devices 114a and 114b to determine relative location of user device 104b with respect to an antenna on network device 114a or 114b. System 100 can combine techniques, such as using signal amplitude differential combined with the phase differential techniques described above to determine location. The location techniques described are not limited to any specific type of antenna technology. System 100 can employ an antenna associated with a wireless access point 120, or an antenna associated with a stand-alone device, including, but not limited to, a personal digital assistant or a laptop computer, designed to relay information to a network-related device employed to calculate relative location from received data. One or more antennas can be deployed in one or more wireless access points 120. System 100 can also vary and limit the transmission strength of the wireless access points 120, so that system 100 can determine and control a radius of relative location based on the radius of operation due to the limited transmission strength. This relative location can be further limited from the radius of operation by other physical barriers such as walls and non-accessible locations within the radius of operation. Roose '556 at 13:16–63 As described above for both wireless and cable-based transmission media, system 100 maintains and updates the location information associated with the connection points (e.g., 160a-i) of the system 100 in a location database. The information included in the location database can vary. For example, Table 1 is a table containing the type of information that can be included in the location database. As illustrated in Table 1, each row represents an association between a connection point and its corresponding location in one or more formats. The “Connection Point ID” column contains the unique identifier associated with a particular connection point. The connection point ID can be any ID that uniquely identifies a connection point. As described in more detail below and illustrated in Table 1, in one example the combination of a device Media Access Control (MAC) address (e.g., 00001d000001) and a port MAC address within the device (e.g., 00001d000101) determines the connection point ID. The locations contained in Table 1 are included in two format types for each connection point ID. The first type is an American National Standards Institute (ANSI) Location Identification Number (LIN) and the second type is a coordinate of latitude and longitude. (Some additional example formats system 100 can employ are described in the alternatives section below.)

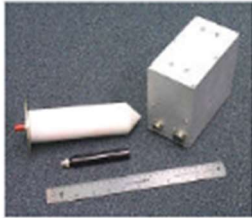
Claims	Prior Art
	Roese '556 at 13:65–14:24 The location information of Table 1 additionally includes the optional parameters “Level of Trust” and “Device ID”. The level of trust, as explained in more detail below, is a parameter with a value in a predefined range, where the range represents the trustworthiness of the location reference. The level of trust generally corresponds with the trustworthiness of the source providing the location of the connection point. A higher level of trust value represents a higher level of confidence that the location reference is accurate, reliable and has neither been altered or generated falsely to gain normally unauthorized access. The device ID uniquely identifies the device that is connected to the connection point. The device ID information enables system 100 to store a map of the physical locations of all the network devices (e.g., 104, 114, 136). This is beneficial if there are devices associated with system 100 that are not configured to acquire and/or store their location information. System 100 can use this corresponding device information to enable location server 134 to transmit location information to a location-aware application since the device cannot transmit the location information itself. IN other words, system 100 can act as a third-party verifier for applications requiring verified location information. Table 1 can include other information in addition or as an alternative to the device ID. For example, Table 1 can include MAC address, address, phone number, protocol type, asset ID, owner and/or the like. Roese '556 at 14:52–64 As described above, once the location database is established, system 100 can provide the location information to a device when that device connects to a connection point. This can include providing location information to devices outside of infrastructure 101 as well as devices within infrastructure 101. FIGS. 2 and 3 illustrate additional examples of system 100 locating devices. FIG. 2 broadly illustrates the steps system 100 performs, from discovering a device's connection to system 100 to allowing the device access to the network. FIG. 3 illustrates more specifically the steps system 100 performs to determine the location of the discovered device. In other words, FIG. 3 shows a portion of the steps of FIG. 2 in more detail. Roese '556 at 14:65–15:17 FIG. 2 broadly illustrates an example of a sequence of steps system 100 performs, from discovering a device's connection to system 100 to allowing the device access to the network. Referring to the example location identification process 201 of FIG. 2, system 100 activates or otherwise discovers (step 210) a device destined for a network association, or a device already network associated. System 100 queries (step 215) the device for location information. That location information may be of absolute or relative type. If location information does not exist, system 100 queries (step 220) whether the device can identify

Claims	Prior Art
	its own location. If the location information does exist, or the device can provide a trustworthy location, system 100 establishes (step 230) the device location information. A location is trustworthy, for example, if the system 100 assigns a level of trust value for that location that is above a predefined threshold. The predefined threshold can vary depending on the network resources that the device requests. For example, sensitive information and applications require a much higher threshold than access to public information. Roese '556 at 16:48–67 Referring to FIG. 3, example process 300 illustrates the steps system 100 performs to determine the location of the discovered device. For clarity and example only, some portions of example process 300 refer to a location server and a location client. A location server refers to a device of system 100 comprising functionality in location module 185 that enables that device to provide location information to another network device. This can include hardware and/or software applications for the storage of location information parameters, access to the storage devices containing values for parameters, algorithms and processes to determine the location of a device and other like functionality. Additionally, location module 185 of a location server may be further configured to provision operational configuration parameters based on the location of the network-attached device, as illustrated in the optional steps of FIG. 3. A location client refers to the device for which the location server is trying to determine location. The network entity of FIG. 3 represents an intermediary device that includes the access port through which the location client communicates. Roese '556 at 23:40–59 In more detail, FIG. 4 illustrates an example process 401 that system 100 employs to determine whether any restrictions to access the network, based on location, are applicable. Specifically, in example location identification process 401 represented by FIG. 4, a user seeking access to system 100 can be first authenticated (step 405) or otherwise filtered by system 100. System 100 achieves this portion of the authorization process by requiring the end user at a location client device to supply certain user information including but not limited to, a name and one or more passwords (e.g., necessary user credentials). If the user is permitted access to system 100 on that basis (e.g., user name and password), system 100 permits the user to query (step 410) system 100 for access to certain information, applications, and the like. Alternatively or in addition, system 100 receives (step 415) the device location before allowing the requested access. A trusted user device (e.g., 104), a network infrastructure device (e.g., a network entry device 114) and/or a location server can supply the user device location using the techniques as described herein.

Claims	Prior Art
	Roese '556 at 26:29–46 Use of the above techniques enables system 100 to restrict access to data, applications, specific networked devices, data and network service, QOS (Quality of Service) levels, network tools, functionality, rules, and the like, based on the user and/or the location of the device associated with the user seeking access. Further to the techniques above, system 100 can employ the location information to effect a modification of the access requirements. For example, when a device seeks network access from a location deemed not to be inherently secure (e.g., such as a public facility like an airport), system 100 can prompt a user to initiate an improved connection, such as a virtual private network (VPN), or can inform the user that supplemental restrictions apply while in the insecure area. More generally, this can be seen as an expansion of policy-based access in that the access rules for an individual user may be adapted as a function of the client device location and/or the level of trust associated with the location information. Roese '556 at 27:29–51 In addition to access control, system 100 can use location information to enforce restrictions regarding the transmission of data. As described in the overview example, location information allows system 100 to deny access to certain sensitive information upon request from a location client outside of a specified region, or to prohibit data from being transmitted through an intermediate device that is located outside of a specified region. FIG. 6 illustrates an example process 601 that system 100 employs to effect these data transmission restrictions. Specifically, in the example information tagging process 601 represented by FIG. 6, system 100 receives (step 605) a request from an end user for access to information (e.g., file, document, and/or the like, generally, data). This assumes that the end user has been adequately authenticated or otherwise permitted access to the network, as described above. System 100 then determines (step 610) whether the requested data is location sensitive. That is, whether the data should not be moved beyond certain defined boundaries (e.g., a present device, a room, a building, a campus, a city, a country and the like). If system 100 determines (step 610) that the data is not location sensitive, system 100 permits (step 615) access to that data that is not restricted by location. Roese '556 at 28:39–57 With a location-aware infrastructure, system 100 can employ trusted location information to provide other services in addition to those described above. For example, system 100 can use the location information in emergency situations, where a device may be an alarm or sensor. System 100 determines the location of the alarm device and transmits the location information to a party responding to the alarm. System 100 can also use location information to recover a stolen user device 104. As the stolen user device 104 accesses system 100, system 100 determines the location of the stolen device and transmits the location

Claims	Prior Art
	information to a party seeking to locate the device. System 100 can track mobile user devices (e.g., 104b) and thus can also track anything associated with that user device (e.g., the user, a file, a physical object, and the like). System 100, through the use of location information, can provide these and other services and applications. The examples that follow illustrate how system 100 can employ location information to provide these and other services and applications. Roose '556 at 30:32–45 Referring to FIG. 8, system 100' provides another example of a location-aware network and is described as an enterprise network that serves as a data communications network for a business organization or other type of enterprise. The enterprise operates the network according to various policies, which may include location-dependent aspects. For example, access-control policies may depend on the locations of devices accessing services on the network. In various configurations, system 100' may include or make use of one or more LANs, MANs, WANs, PANs and/or Ethernet to the first mile (e.g., IEEE 802.3ah). In other examples of such a network, the physical and logical arrangement of the devices can differ from that shown in FIGS. 1 and 8. Roose '556 at 31:31–48 Network entry devices 114 and end user devices 104 can come in a wide array of configurations. For example, user devices 104 can include individual computers, printers, servers, cellular phones, laptops, handheld electronic devices, telephones, Internet Protocol (IP)-configured telephones, switch devices, and the like. Network entry devices 114 can include, for example, switches, routers, hubs, bridges, repeaters, wireless access points, data communications equipment, server computers, modems, multiplexers, Private Branch Exchanges (PBXs), virtually any devices used to interconnect data equipment or end devices, and the like. The discreet boundaries of infrastructure 101' are for illustration only. For example, system 100' may include a server outside of the illustrated boundary while remaining logically part of infrastructure 101'. In another example, there may be a portion of network infrastructure 101' connected to system 100' located in a remote network, such as Internet 148. Roose '556 at 35:30–41 One example of automated network management employing the location advertising system is the configuration of Voice over IP handsets with a neighbor discovery protocol in a data network. Voice over IP handsets typically are designed to communicate with Ethernet switches and can require complex configurations. Networks with the location advertising system can integrate neighbor discovery protocols with Voice over IP handsets to provide configuration information to the handset, discover inventory

Claims	Prior Art
	information to be stored on the connection point switch, and automatically configure the ports' parameters on the connection point switch/access platform. Mandke 2003A at 11 Some of the applications IEEE 802.15.3a anticipates supporting are: Voice over IP, HDTV, Home Theater, digital imaging, and location awareness. In March 2003, Task Group 802.15.3a heard the first round of presentations out of the 29 respondents to the CFP (Appendix B) for higher data rate physical layer alternatives to the physical layer in the 802.15.3 standard (55 Mbps in the 2.4 GHz ISM band). The standard being developed by IEEE 802.15.3a will replace the physical layer for IEEE 802.15.3 (i.e. it will use the same media-access control layer as the IEEE 802.15.3 standard). The IEEE is expected to publish the approved standard in mid-2004. Mandke 2003A at 12 Location awareness improves the usability of portable devices. A specific device can be located and identified amongst users in crowded environments. This greatly simplifies device registration in ad-hoc networks. Provisions must be made to propagate location information to a suitable management entity. Fontana at 5 Ultra wideband technology was considered for this application because of its ability to transmit large amounts of data at high speed in a mobile, multipath-prone environment. The UWB tag operated in the L-band region (1.4 to 1.65 GHz) and had a peak output power of approximately 250 mW for a demonstrated range of over 300 meters. The image of the driver was stored as a compressed JPEG file, together with additional ASCII data, in EEPROM and periodically transmitted at a 400 kb/s burst rate to a UWB receiver with display. The tag operated off of two AAA batteries (3.0V) and, in an operational scenario, was mounted behind the front grill of the automobile.

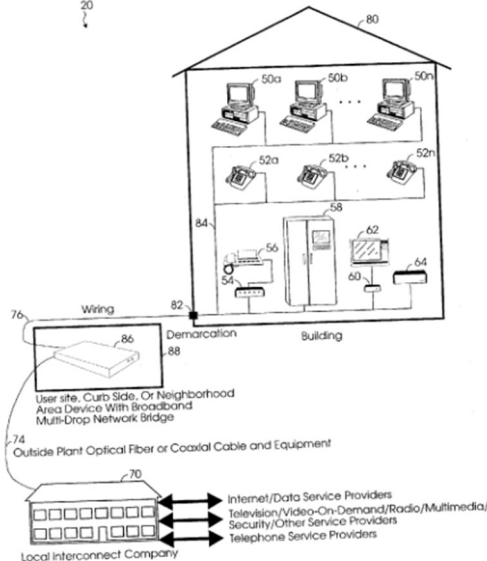
Claims	Prior Art
	Fontana at Figure 8  Figure 8. UWB Precision Geolocation System Transceiver. Fontana at 6 The system in Figure 8 utilizes a 2.5 ns, 4 Watt peak, UWB pulse, again operating in the 1.3 to 1.7 GHz region. Line-of-sight range for the system is better than 2 kilometers utilizing small, omnidirectional vertically polarized (smaller) or circularly polarized (larger) antennas. Within a building, the range becomes limited by wall and obstacle attenuation; however, ranges exceeding 100 meters inside have been attained. An unique feature of the system is the ability to detect the pulse leading edge through the use of a charge sensitive, tunnel diode detector. Leading edge detection is critical to the resolution of the direct path from the plethora of multipath returns produced from internal reflections. The UWB geolocation system was originally developed to permit a soldier to determine his or her position to within 1 foot resolution in an urban environment. It is currently being used to augment a video capture system for 3-D modeling, and for materiel location onboard a Navy ship. Fontana at Figure 10  Figure 10. UWB Backup Sensor. Fontana at 7 Several variants of the Hummingbird radar have also been developed. For example, Figure 10 illustrates an ultra wideband backup sensor for the detection of personnel, vehicles and other objects behind large construction and mining vehicles.

Claims	Prior Art
	[Figure 10] Operating with approximately 250 mW peak in the C-band region from 5.4 to 5.9 GHz, the backup sensor utilizes a dual antenna configuration for the detection of objects as close as 1 foot to beyond 350 feet from the vehicle. Ultra wideband provides a significant advantage for this application because of the ability to provide precision range gating to eliminate clutter which, with conventional Doppler-based sensors, often results in large false alarm rates. This sensor was developed for the National Institute of Occupational Safety and Health. Discrete Time Proposal at Slide 5 Summary • Compliant with FCC 02-48, UWB Report & Order • 3.1-10.6GHz, 500MHz band spacing • Varies symbol rate and number of bands, from 16Mbps to 600Mbps at PHY-SAP • Scalable down to lower bit rates for lower power, lower cost • Due to time constraints this presentation addresses – Frequency plan – Modulation scheme – Performance in AWGN channel – MAC considerations – Location awareness (contribution from Uri Kareev, Pulsicom) – Concepts of pulse shaping and multiple access • Remaining material will be presented at the next opportunity in May 2003 – Performance in multipath – Channelization – Implementation feasibility – Self evaluation criteria – Other issues that will emerge from group's feedback Melick '146 at 8:11–16 According to one aspect of the present invention, the present invention provides for storing data by persistently maintaining the data on a network, through retransmission. The data can be associated with expiration properties. The expiration properties can include geographical information and/or time attributes. The data can be in packets or streams.
[1h] wherein said controller is configured or configurable to	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said controller is configured or configurable to perform or for performing at least one of:

Claims	Prior Art
perform or for performing at least one of: a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources; and b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources.	a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources; and b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said controller is configured or configurable to perform or for performing at least one of: a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources; and b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said controller is configured or configurable to perform or for performing at least one of: a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources; and b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one radio to another via an intermediate repeater link. Malan '698 at Abstract A method and system are provided for protecting publicly accessible network computer services from

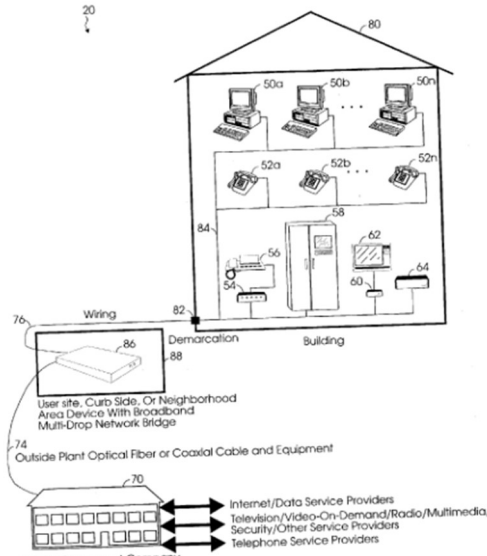
Claims	Prior Art
	undesirable network traffic in real-time. The method includes receiving network traffic destined for the services and analyzing the network traffic to identify an undesirable user of the services. Access of the undesirable user to the services is limited to protect the services. The method and system identify and remove a new level of security threat that is not addressable by current techniques. Specifically, the method and system identify topologically anomalous application-level patterns of traffic and remove these data flows in real-time from the network. Malan '698 at [0022] An object of the present invention is to provide a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time. Malan '698 at [0023] In carrying out the above objects and other objects of the present invention, a method for protecting publicly accessible network computer services from undesirable network traffic in real-time is provided. The method includes receiving network traffic destined for the services, and analyzing the network traffic to identify an undesirable user of the services. The method further includes limiting access of the undesirable user to the services to protect the services. Malan '698 at [0051] In general, the present invention provides a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time and is useful within a larger system which combats denial of service attacks without requiring any changes to the existing Internet routing infrastructure. This larger system, in general, combines network topology information and coarse-grained traffic statistics from routers to detect, backtrack, and filter distributed attacks on enterprise networks and websites. This larger system exploits information from routers without requiring any changes to the existing Internet routing infrastructure. The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and enterprise networks. The method and system is enabled by functionality that the major routing vendors have put into their latest products. Zuk '399 at [0052] Intruding packets are detected and prevented from spreading to the private or outside networks by the protocol anomaly detection, stateful signature detection, and traffic signature detection software modules.

Claims	Prior Art
	Intruding packets are those containing network attack identifiers associated with network security breaches. Such network attack identifiers may be protocol irregularities, attack signatures, traffic signatures, or a combination of one or more of these, among others. The protocol anomaly detection module looks at the packet flows arranged by the flow manager software module to determine irregularities in the network protocol specifications in the packet. The stateful signature detection module matches known attack signatures to the TCP data stream in case of TCP packets and to the headers and data of packets transmitted with other network protocols. The traffic signature module matches traffic signatures to the network traffic to detect attacks such as port scans and network sweeps. Incoming packets that are judged malicious are dropped by the sensor before reaching any of the network hosts and likewise, outgoing packets are dropped by the sensor before reaching the outside network. The sensor may also drop all the packets in a given session if one or more of its packets are considered to be malicious.
2. The broadband wireless repeater or relay of claim 1, wherein at least one of said one or more network backbones to which said controller is connected or connectable is a wired backbone.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[T]he broadband wireless repeater or relay of claim 1, wherein at least one of said one or more network backbones to which said controller is connected or connectable is a wired backbone.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[T]he broadband wireless repeater or relay of claim 1, wherein at least one of said one or more network backbones to which said controller is connected or connectable is a wired backbone” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[T]he broadband wireless repeater or relay of claim 1, wherein at least one of said one or more network backbones to which said controller is connected or connectable is a wired backbone” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Engels ’850 at 9:16–26 Generally the second antenna means (10) of the indoor to outdoor coupling unit can be a) an omnidirectional antenna (10, Fig. 6a), b) a directive antenna (10) having a 3dB bandwidth over a limited angle in the azimuth plane, e.g. a half-sphere, and directed towards the outside of the building (Fig. 6b), or c) a directional antenna (10) having a 3dB bandwidth angle less than 180°, e.g. 60° or 90°, pointed to the outdoor antenna (Fig. 6c). In the latter case, due to the larger antenna gain, a higher signal attenuation can be accommodated and the length of the transmission path (6) can be larger. However, such a directional antenna needs usually to be pointed towards the outdoor antenna (9), e.g. manually. Alternatively, the second antenna means may be replaced by connection (30) to a cable network such as an optical fibre

Claims	Prior Art
	cable, a coax cable, a twisted pair cable or similar (Fig. 6d). Bareis '373 at FIG. 2  FIG. 2 Bareis '373 at [0036] Referring now to FIG. 1, there is illustrated a first embodiment of a broadband multidrop local network 10 consistent with the present disclosure. Typically, network 10 may include a twisted-pair wire bus as exists in the outside plant 72 of a local interconnect company 70, such as a telephone company local exchange carrier (LEC), cable company office, or the like. Alternatively, the outside plant media could consist of coaxial cable in a cable network. It is also conceivable that optical versions of the embodiments of the present disclosure could be deployed using optical fiber to transport the data in the network. Bareis '373 at [0042] Referring now to FIG. 2, there is illustrated an alternate embodiment of the present disclosure directed to a very high speed data throughput. Very high speed data throughput has greater applicability in video-on-demand and video distribution applications, very fast Internet access, video telephony, and the like. In FIG. 2, a building 80 contains at least one network device to be connected via twisted-pair wire 84 to Local Interconnect Company 70 through demarcation point 82, thence via a short run of outside plant

Claims	Prior Art
	wiring 76, through a broadband multidrop local network interface 86, and finally through an outside plant optical fiber or coaxial cable 74. Devices that may be used on the network 20 must be compatible with the network interface 400 as will be described hereinbelow in conjunction with FIGS. 4 and 5. Such network devices may include, but are not limited to, computer systems 50 (a) . . . (n), telephone sets 52 (a) . . . (n), digital set top equipment 60, loop-start interface equipment 54, network-ready appliances 58, and security systems 64. Although not shown, other network devices such as television sets, high fidelity audio equipment, DVD or VCR devices, security cameras, utility metering equipment, facsimile machines, etc. each having a built-in network interface 400 may also be connected to the network 20. As described hereinabove, the local interconnect company 70 distributes packetized IP traffic between various service providers and the user site. Bareis '373 at [0058] In the configuration of FIG. 4, IP-based telephone set 52 is used to place and receive Voice over Internet Protocol (VoIP) calls through a service provider via optical fiber 74, broadband multidrop local network interface 86, and the copper wiring 72 and 84 interconnected at Demarcation 82. Bareis '373 at [0097] To summarize, there has been disclosed a broadband multidrop local network architecture for use in intercoupling multimedia traffic to and from a wide variety of addressable network devices. Each network device may be coupled via a network interface or broadband transceiver to a single wireline coupled to an external broadband communication service. Such communication service may be provided, e.g., via fiber optic link to a curbside terminal by an interconnection company, without requiring a complete secondary network and the associated equipment such as modems, routers, converters, hubs, switches, etc. The full data traffic capability at the full bandwidth achievable with relatively short runs (e.g., on the order of 100 meters) of twisted pair copper wire may be utilized when all traffic for all of the participating network devices is packetized on a wired medium for distribution thereon without the bandwidth, point-to-point, or data rate restrictions associated with conventional individual DSL (digital subscriber line) or similar services. In effect, the useable spectrum that exists on the broadband multidrop local network as disclosed hereinabove is a closed spectrum; that is, the entire bandwidth technically feasible on a twisted-pair medium over these relatively short distances is dedicated to the broadband communication capability implemented in each local network such that total data rates, with present standards and technologies, of at least 100 Mbps, and beyond to over 500 Mbps at reasonable distances, are available for each local network transferring data packets at the maximum packet rate of all network devices attachable thereto even when all of the network devices are transmitting. Each network device (computers, peripherals,

Claims	Prior Art
	telecommunications equipment, security systems, broadcast audio and video, to name just a few) may be assigned a bandwidth or packet data rate rating such that its use on the network appropriates a required portion of the total available data traffic capabilities of the network when in use and the user knows immediately what portion of his/her network capacity is being utilized. Roose '556 at 1:38–47 Computing systems are useful tools for the exchange of information among individuals. The information may include, but is not limited to, data, voice, graphics, and video. The exchange is established through interconnections linking the computing systems together in a way that permits the transfer of electronic signals that represent the information. The interconnections may be either cable or wireless. Cable connections include, for example, metal and optical fiber elements. Wireless connections include, for example infrared, acoustic, and radio wave transmissions.
3. The broadband wireless repeater or relay of claim 2, wherein said wired backbone is selected from a group consisting of T1, T3, DSL, cable, cable modem, fiber, optical cable, copper lines, coax, phone, ethernet, and internet.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 2, wherein said wired backbone is selected from a group consisting of T1, T3, DSL, cable, cable modem, fiber, optical cable, copper lines, coax, phone, ethernet, and internet.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 2, wherein said wired backbone is selected from a group consisting of T1, T3, DSL, cable, cable modem, fiber, optical cable, copper lines, coax, phone, ethernet, and internet” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 2, wherein said wired backbone is selected from a group consisting of T1, T3, DSL, cable, cable modem, fiber, optical cable, copper lines, coax, phone, ethernet, and internet” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Engels '850 at 9:16–26 Generally the second antenna means (10) of the indoor to outdoor coupling unit can be a) an omnidirectional antenna (10, Fig. 6a), b) a directive antenna (10) having a 3dB bandwidth over a limited angle in the azimuth plane, e.g. a half-sphere, and directed towards the outside of the building (Fig. 6b), or c) a directional antenna (10) having a 3dB bandwidth angle less than 180°, e.g. 60° or 90°, pointed to the outdoor antenna (Fig. 6c). In the latter case, due to the larger antenna gain, a higher signal attenuation can be accommodated and the length of the transmission path (6) can be larger. However, such a directional

Claims	Prior Art
	antenna needs usually to be pointed towards the outdoor antenna (9), e.g. manually. Alternatively, the second antenna means may be replaced by connection (30) to a cable network such as an optical fibre cable, a coax cable, a twisted pair cable or similar (Fig. 6d). Bareis '373 at FIG. 2  FIG. 2 Bareis '373 at [0036] Referring now to FIG. 1, there is illustrated a first embodiment of a broadband multidrop local network 10 consistent with the present disclosure. Typically, network 10 may include a twisted-pair wire bus as exists in the outside plant 72 of a local interconnect company 70, such as a telephone company local exchange carrier (LEC), cable company office, or the like. Alternatively, the outside plant media could consist of coaxial cable in a cable network. It is also conceivable that optical versions of the embodiments of the present disclosure could be deployed using optical fiber to transport the data in the network. Bareis '373 at [0038] Referring further to FIG. 1, a building 80 contains a number of addressable network devices to be networked via interconnecting twisted-pair wire 84 to the local interconnect company 70 via the demarcation point 82 and the outside plant wiring 72. Devices that may be used on the network 10 must

Claims	Prior Art
	be compatible with the network transceiver 400 as shown in FIGS. 4 and 5 to be described hereinbelow. Such network devices may include, but are not limited to, computer systems 50 (a) . . . (n), telephone sets 52 (a) . . . (n), digital set top equipment 60, loop-start interface equipment 54, network-ready appliances 58, and security systems 64. Although not shown, other network devices such as television sets, high fidelity audio equipment, DVD or VCR devices, security cameras, utility metering equipment, facsimile machines, etc., each having a built-in addressable network interface 400, may also be connected to the network 10. Bareis '373 at [0039] The local interconnect company 70 distributes packetized IP traffic such as the well-known Internet protocol (IP) for computers, or voice over Internet protocol (VoIP) for telephony, between various service providers and the user site. For another example, IP-based television broadcast service data distributed as streaming data can be routed to set top equipment 60 to be converted to video and audio signals compatible with a television set 62. In this example, a single television set 62 and set top equipment 60 are shown. In actual implementations, one or more of each device may be used and the functions of television set 62 and set top equipment 60 may be integrated into a single device. Another example is the routing of digitized and packetized telephony traffic between a telephone company service provider and at least one telephone set 52. The telephone company service provider may provide long distance capabilities, local calling capabilities or a combination thereof. Still another example consists of computers 50 (a) . . . (n) connected to the network 10. The computers 50 (a) . . . (n) may intercommunicate using IP packets or communicate to and from at least one Internet service provider operating through a local interconnect company 70. Yet another example is the routing of data traffic to communicate between the user site and security services. The examples given are illustrative of the many possible uses for the network of the present disclosure and are not intended to be limiting. Bareis '373 at [0042] Referring now to FIG. 2, there is illustrated an alternate embodiment of the present disclosure directed to a very high speed data throughput. Very high speed data throughput has greater applicability in video-on-demand and video distribution applications, very fast Internet access, video telephony, and the like. In FIG. 2, a building 80 contains at least one network device to be connected via twisted-pair wire 84 to Local Interconnect Company 70 through demarcation point 82, thence via a short run of outside plant wiring 76, through a broadband multidrop local network interface 86, and finally through an outside plant optical fiber or coaxial cable 74. Devices that may be used on the network 20 must be compatible with the network interface 400 as will be described hereinbelow in conjunction with FIGS. 4 and 5. Such network

Claims	Prior Art
	devices may include, but are not limited to, computer systems 50 (a) . . . (n), telephone sets 52 (a) . . . (n), digital set top equipment 60, loop-start interface equipment 54, network-ready appliances 58, and security systems 64. Although not shown, other network devices such as television sets, high fidelity audio equipment, DVD or VCR devices, security cameras, utility metering equipment, facsimile machines, etc. each having a built-in network interface 400 may also be connected to the network 20. As described hereinabove, the local interconnect company 70 distributes packetized IP traffic between various service providers and the user site. Bareis '373 at [0058] In the configuration of FIG. 4, IP-based telephone set 52 is used to place and receive Voice over Internet Protocol (VoIP) calls through a service provider via optical fiber 74, broadband multidrop local network interface 86, and the copper wiring 72 and 84 interconnected at Demarcation 82. Bareis '373 at [0097] To summarize, there has been disclosed a broadband multidrop local network architecture for use in intercoupling multimedia traffic to and from a wide variety of addressable network devices. Each network device may be coupled via a network interface or broadband transceiver to a single wireline coupled to an external broadband communication service. Such communication service may be provided, e.g., via fiber optic link to a curbside terminal by an interconnection company, without requiring a complete secondary network and the associated equipment such as modems, routers, converters, hubs, switches, etc. The full data traffic capability at the full bandwidth achievable with relatively short runs (e.g., on the order of 100 meters) of twisted pair copper wire may be utilized when all traffic for all of the participating network devices is packetized on a wired medium for distribution thereon without the bandwidth, point-to-point, or data rate restrictions associated with conventional individual DSL (digital subscriber line) or similar services. In effect, the useable spectrum that exists on the broadband multidrop local network as disclosed hereinabove is a closed spectrum; that is, the entire bandwidth technically feasible on a twisted-pair medium over these relatively short distances is dedicated to the broadband communication capability implemented in each local network such that total data rates, with present standards and technologies, of at least 100 Mbps, and beyond to over 500 Mbps at reasonable distances, are available for each local network transferring data packets at the maximum packet rate of all network devices attachable thereto even when all of the network devices are transmitting. Each network device (computers, peripherals, telecommunications equipment, security systems, broadcast audio and video, to name just a few) may be assigned a bandwidth or packet data rate rating such that its use on the network appropriates a required portion of the total available data traffic capabilities of the network when in use and the user knows

Claims	Prior Art
	immediately what portion of his/her network capacity is being utilized. Roose '556 at 1:38–47 Computing systems are useful tools for the exchange of information among individuals. The information may include, but is not limited to, data, voice, graphics, and video. The exchange is established through interconnections linking the computing systems together in a way that permits the transfer of electronic signals that represent the information. The interconnections may be either cable or wireless. Cable connections include, for example, metal and optical fiber elements. Wireless connections include, for example infrared, acoustic, and radio wave transmissions.
6. The broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform a).	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform a).” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform a)” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform a)” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one

Claims	Prior Art
	radio to another via an intermediate repeater link. Malan '698 at Abstract A method and system are provided for protecting publicly accessible network computer services from undesirable network traffic in real-time. The method includes receiving network traffic destined for the services and analyzing the network traffic to identify an undesirable user of the services. Access of the undesirable user to the services is limited to protect the services. The method and system identify and remove a new level of security threat that is not addressable by current techniques. Specifically, the method and system identify topologically anomalous application-level patterns of traffic and remove these data flows in real-time from the network. Malan '698 at [0022] An object of the present invention is to provide a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time. Malan '698 at [0023] In carrying out the above objects and other objects of the present invention, a method for protecting publicly accessible network computer services from undesirable network traffic in real-time is provided. The method includes receiving network traffic destined for the services, and analyzing the network traffic to identify an undesirable user of the services. The method further includes limiting access of the undesirable user to the services to protect the services. Malan '698 at [0051] In general, the present invention provides a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time and is useful within a larger system which combats denial of service attacks without requiring any changes to the existing Internet routing infrastructure. This larger system, in general, combines network topology information and coarse-grained traffic statistics from routers to detect, backtrack, and filter distributed attacks on enterprise networks and websites. This larger system exploits information from routers without requiring any changes to the existing Internet routing infrastructure. The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and enterprise networks. The method and system is enabled by functionality that the major routing vendors

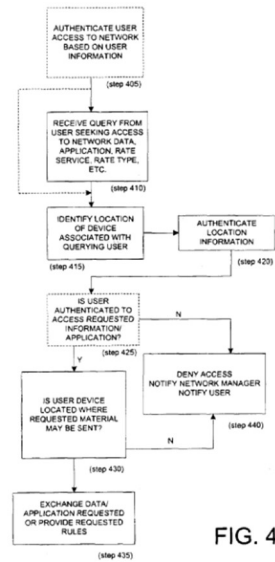
Claims	Prior Art
	have put into their latest products. Zuk '399 at [0052] Intruding packets are detected and prevented from spreading to the private or outside networks by the protocol anomaly detection, stateful signature detection, and traffic signature detection software modules. Intruding packets are those containing network attack identifiers associated with network security breaches. Such network attack identifiers may be protocol irregularities, attack signatures, traffic signatures, or a combination of one or more of these, among others. The protocol anomaly detection module looks at the packet flows arranged by the flow manager software module to determine irregularities in the network protocol specifications in the packet. The stateful signature detection module matches known attack signatures to the TCP data stream in case of TCP packets and to the headers and data of packets transmitted with other network protocols. The traffic signature module matches traffic signatures to the network traffic to detect attacks such as port scans and network sweeps. Incoming packets that are judged malicious are dropped by the sensor before reaching any of the network hosts and likewise, outgoing packets are dropped by the sensor before reaching the outside network. The sensor may also drop all the packets in a given session if one or more of its packets are considered to be malicious.
8. The broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform network provisioning or monitoring.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform network provisioning or monitoring.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform network provisioning or monitoring” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 1, wherein said controller is configured to or configurable to perform network provisioning or monitoring” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success.

Claims

Prior Art

Roose '556 at FIG> 4

501



Claims

Prior Art

Roose '556 at FIG. 5

500

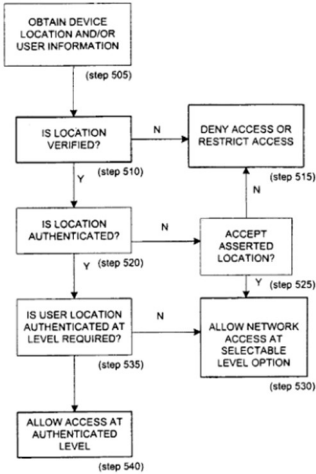
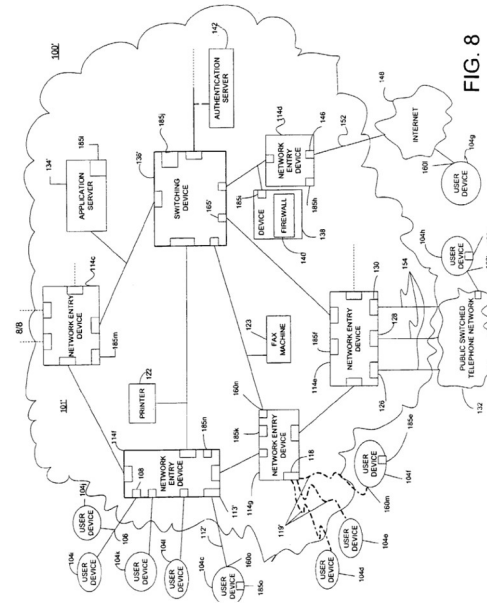


FIG. 5

Claims	Prior Art
	Roese '556 at FIG. 8  Roese '556 at 19:29–67 One type of automated mechanisms involves the provisioning and configuration of devices as they are added to system 100. When added, system 100 determines the location of the added device and then based on that location, system 100 determines, for example, what particular configuration file should be loaded into the device, what type of network priorities the device should be assigned, such as bandwidth, latency, QoS and other like network policies. This mechanism enables system 100 to enforce any of these policies based on the location of each device. The examples that follow illustrate how system 100 can expand data within the location database to include the provisioning and/or configuration data. Roese '556 at 20:3–32 In one specific example of provisioning, a location server assigns location information and network specific configurations to Voice over IP (VoIP) handsets. The information is provisioned on the phone and includes, for example, Virtual LANs (VLANs) ID, traffic prioritization at layer 2 or layer 3, and an E911 LIN. This simplifies the information on VoIP phones in branch offices, for example. The provisioned parameters are added to the location information in the location database of the location server. An expanded location database for VoIP phone environments can include the following

Claims	Prior Art
	information: VLAN membership of the voice entity, layer 2 priority mappings for voice payload/voice control/non voice traffic, layer 3 class of service markings for voice payload/voice control/non voice traffic, location client's network layer address, ANSI LIN numbering, geographic location information including latitude, longitude, altitude and accuracy factor, device microcode file to boot (e.g., bootp server pointer), and/or other like parameters. Table 2 is a table containing an example of the type of information that can be included in an expanded location database that includes additional provisioning parameters for a VoIP network. In addition to the connection point ID and the location reference, the location database represented by Table 2 also includes a voice VLAN ID and a voice priority parameter. As described above, the location database also can include device ID data about a location client. In the VoIP example, these optional device ID parameters can include the handset extension number, the handset model number, the handset version, the handset network address, and/or the like. Roese '556 at 26:29–46 Use of the above techniques enables system 100 to restrict access to data, applications, specific networked devices, data and network service, QOS (Quality of Service) levels, network tools, functionality, rules, and the like, based on the user and/or the location of the device associated with the user seeking access. Further to the techniques above, system 100 can employ the location information to effect a modification of the access requirements. For example, when a device seeks network access from a location deemed not to be inherently secure (e.g., such as a public facility like an airport), system 100 can prompt a user to initiate an improved connection, such as a virtual private network (VPN), or can inform the user that supplemental restrictions apply while in the insecure area. More generally, this can be seen as an expansion of policy-based access in that the access rules for an individual user may be adapted as a function of the client device location and/or the level of trust associated with the location information. Roese '556 at 27:29–51 In addition to access control, system 100 can use location information to enforce restrictions regarding the transmission of data. As described in the overview example, location information allows system 100 to deny access to certain sensitive information upon request from a location client outside of a specified region, or to prohibit data from being transmitted through an intermediate device that is located outside of a specified region. FIG. 6 illustrates an example process 601 that system 100 employs to effect these data transmission restrictions. Specifically, in the example information tagging process 601 represented by FIG. 6, system 100 receives (step 605) a request from an end user for access to information (e.g., file, document, and/or the like, generally, data). This assumes that the end user has been adequately authenticated or otherwise permitted access to the network, as described above. System 100 then

Claims	Prior Art
	determines (step 610) whether the requested data is location sensitive. That is, whether the data should not be moved beyond certain defined boundaries (e.g., a present device, a room, a building, a campus, a city, a country and the like). If system 100 determines (step 610) that the data is not location sensitive, system 100 permits (step 615) access to that data that is not restricted by location. Roose '556 at 28:39–57 With a location-aware infrastructure, system 100 can employ trusted location information to provide other services in addition to those described above. For example, system 100 can use the location information in emergency situations, where a device may be an alarm or sensor. System 100 determines the location of the alarm device and transmits the location information to a party responding to the alarm. System 100 can also use location information to recover a stolen user device 104. As the stolen user device 104 accesses system 100, system 100 determines the location of the stolen device and transmits the location information to a party seeking to locate the device. System 100 can track mobile user devices (e.g., 104b) and thus can also track anything associated with that user device (e.g., the user, a file, a physical object, and the like). System 100, through the use of location information, can provide these and other services and applications. The examples that follow illustrate how system 100 can employ location information to provide these and other services and applications. Roose '556 at 30:32–45 Referring to FIG. 8, system 100' provides another example of a location-aware network and is described as an enterprise network that serves as a data communications network for a business organization or other type of enterprise. The enterprise operates the network according to various policies, which may include location-dependent aspects. For example, access-control policies may depend on the locations of devices accessing services on the network. In various configurations, system 100' may include or make use of one or more LANs, MANs, WANs, PANs and/or Ethernet to the first mile (e.g., IEEE 802.3ah). In other examples of such a network, the physical and logical arrangement of the devices can differ from that shown in FIGS. 1 and 8. Mandke 2003A at 11 Interference susceptibility refers to the impact that other co-located intentional and unintentional radiators may have on the alt-PHY. The error rate criterion is the maximum packet error rate (PER).

Claims	Prior Art
	Mandke 2003A at 11 The PER should be less than 8% for a 1024 byte packet length when an interferer is present at a separation of 1m from the receiver. A broad representative set of interferers such as WLANs (2.4 GHz and 5 GHz), other WPANs (such as 802.15.1, 802.15.3, and 802.15.4), ISM cordless phones (2.4 GHz and 5 GHz), and radiators such as microwave ovens are the primary cases considered. Mandke 2003A at 11–12 Coexistence refers to the co-location of IEEE P802.15.3a devices with other, non-802.15.3a devices. The 802.15.3a devices must coexist with other receivers such as Bluetooth™ (IEEE 802.15.1), 802.15.3, IEEE 802.11b, IEEE 802.11a, and IEEE 802.15.4 that operate in the unlicensed spectrum and which may be co-located with 802.15.3a devices. The minimum criteria here is that the interfering average power generated by the 802.15.3a transmitter and measured in the relevant bandwidth of the victim receiver should be at least 6 dB below the minimum sensitivity level of the non-802.15.3a device operating in the 6 Mbps mode, when the separation between the 802.15.3a transmitter and victim receiver is 1 m. Mandke 2003A at 13 The signal acquisition methods are the techniques by which the proposed receiver acquires and tracks the incoming signal in order to correctly receive the transmitted data. Target acquisition times are less than 6 μs for piconet clear channel assessment (CCA) (referenced to the beginning of the preamble), and less than 20μs for acquisition from the beginning of the preamble to the beginning of the header. Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one

Claims	Prior Art
	radio to another via an intermediate repeater link. Aiello '273 at [0040] Decentralized network 100 also allows uncontrolled deployment of devices, automatic topology management of devices, overlapping network, fair access to burst and priority traffic, and QoS support. Unlike a centralized network, decentralized network 100 does not require a master device to act as a scheduler for traffic. Aiello '273 at [0054] Referring back to FIG. 3, the processor in the transmitting device generates the payload for the packet in step 330. In a preferred embodiment, the payload is Protocol Data Unit (PDU). FIG. 7 illustrates a block diagram of a payload 510 of packet 500 (FIG. 5). In PDU 510, there is a PDU header 700 that includes PDU addressing field 705, sequence number field 710 and parameters field 715. PDU addressing field 705 includes addressing information. Sequence number 710 stores the sequence number of the packet in the packets being transmitted. Parameters field 715 stores original QoS parameters and residual lifetime parameters for use by the receiving device. Data field 720 stores the data being transmitted. Mandke 2003B at 24 The IEEE 802.15.3 task group is developing WPANs up to 55 Mbps. The draft standard operates on five 15 MHz channels in the 2.4 GHz ISM band, two of which interfere with IEEE 802.11b traffic. Modulation (QPSK, DQPSK, 16/32/64-QAM) and coding (trellis-coded modulation) are varied to provide five data rates (11 Mbps, 22 Mbps, 33 Mbps, 44 Mbps, and 55 Mbps) [5]. The MAC layer described by this standard allows for the coordination of WPAN devices to form piconets. The MAC layer also allows for multimedia quality of service (QoS), power management, and ad-hoc networking support. IEEE 802.15.3 gained sponsor ballot approval in May 2003. The focus of UWB occurs in a separate task group, IEEE 802.15.3.a, which is discussed below. Zuk '399 at Abstract Systems and methods for detecting and preventing network security breaches are described. The systems and methods present a gateway-based packet-forwarding network security solution to not only detect security breaches but also prevent them by directly dropping suspicious packets and connections. The systems and methods employ multiple techniques to detect and prevent network security breaches,

Claims	Prior Art
	including stateful signature detection, traffic signature detection, and protocol anomaly detection. Zuk '399 at [0001] This invention relates generally to network security systems and methods for detecting and preventing security breaches on a network. More specifically, the present invention provides gateway-based packet-forwarding network security systems and methods to not only detect security breaches on the network but also prevent them by directly dropping suspicious packets and connections. These systems and methods employ multiple techniques to detect and prevent intrusions, including stateful signature detection, traffic signature detection, and protocol anomaly detection. Zuk '399 at [0009] The security of a private network having a packet filtering firewall may be increased by using Network Address Translation (“NAT”) within the firewall. NAT functions like a private branch exchange in a telephone system. All the source addresses of outgoing IP packets are rewritten to the IP address assigned to the firewall to give the impression that the packets originated from the firewall rather than from the internal hosts of the private network protected by the firewall. Reply packets coming back are translated and forwarded to the appropriate host. With NAT, internal hosts are allowed to connect to hosts outside of the firewall but outside hosts cannot connect directly to the internal hosts since they are only aware of the IP address of the firewall. Zuk '399 at [0010] Packet filtering firewalls are relatively inexpensive and do not interfere with network performance, but alone they cannot typically provide adequate security. Packet filtering rules become unmanageable in complex environments, provide no user authentication mechanisms, and are vulnerable to attacks such as IP spoofing. For example, if a hacker can figure out a trusted IP address, the hacker may forge an IP header to a harmful packet. Being unable to differentiate between a valid packet and a forged one, a packet filtering firewall would not reject the harmful packet.
9[pre]. The broadband wireless repeater or relay of claim 8, wherein the network provisioning or monitoring includes one or more of:	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 8, wherein the network provisioning or monitoring includes one or more of.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he

Claims	Prior Art
	broadband wireless repeater or relay of claim 8, wherein the network provisioning or monitoring includes one or more of” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 8, wherein the network provisioning or monitoring includes one or more of” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 1[pre].</i>
[9a] i) bandwidth or delay provisioning of repeated or relayed transmissions,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “i) bandwidth or delay provisioning of repeated or relayed transmissions.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “i) bandwidth or delay provisioning of repeated or relayed transmissions” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “i) bandwidth or delay provisioning of repeated or relayed transmissions” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
[9b] ii) application prioritization,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “ii) application prioritization.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “ii) application prioritization” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “ii) application prioritization” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
[9c] iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth, and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “iii) prioritizing, delaying or altering of data transmissions,

Claims	Prior Art
	traffic, or bandwidth” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
[9d] iv) monitoring or measuring traffic from one or more devices, users or networks.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “iv) monitoring or measuring traffic from one or more devices, users or networks.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “iv) monitoring or measuring traffic from one or more devices, users or networks” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “iv) monitoring or measuring traffic from one or more devices, users or networks” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Roose ’556 at FIG> 4 501 <pre> graph TD 405[AUTHENTICATE USER ACCESS TO NETWORK BASED ON USER INFORMATION (step 405)] --> 410[RECEIVE QUERY FROM USER SEEKING ACCESS TO NETWORK DATA, APPLICATION, RATE, SERVICE, RATE TYPE, ETC. (step 410)] 410 --> 415[IDENTIFY LOCATION OF DEVICE ASSOCIATED WITH QUERYING USER (step 415)] 415 --> 420[AUTHENTICATE LOCATION INFORMATION (step 420)] 420 --> 425{IS USER AUTHENTICATED TO ACCESS REQUESTED INFORMATION APPLICATION? (step 425)} 425 -- N --> 440[DENY ACCESS NOTIFY NETWORK MANAGER NOTIFY USER (step 440)] 425 -- Y --> 430{IS USER DEVICE LOCATED WHERE REQUESTED MATERIAL MAY BE SENT? (step 430)} 430 -- N --> 440 430 -- Y --> 435[EXCHANGE DATA APPLICATION REQUESTED OR PROVIDE REQUESTED RULES (step 435)] </pre> FIG. 4

Claims

Prior Art

Roose '556 at FIG. 5

500

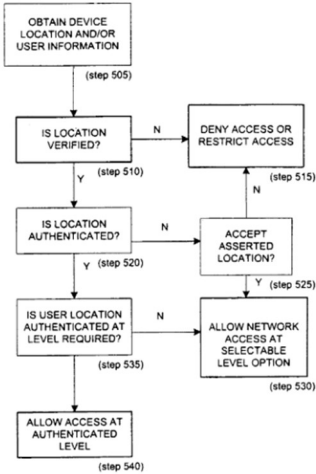


FIG. 5

Claims	Prior Art
	information: VLAN membership of the voice entity, layer 2 priority mappings for voice payload/voice control/non voice traffic, layer 3 class of service markings for voice payload/voice control/non voice traffic, location client's network layer address, ANSI LIN numbering, geographic location information including latitude, longitude, altitude and accuracy factor, device microcode file to boot (e.g., bootp server pointer), and/or other like parameters. Table 2 is a table containing an example of the type of information that can be included in an expanded location database that includes additional provisioning parameters for a VoIP network. In addition to the connection point ID and the location reference, the location database represented by Table 2 also includes a voice VLAN ID and a voice priority parameter. As described above, the location database also can include device ID data about a location client. In the VoIP example, these optional device ID parameters can include the handset extension number, the handset model number, the handset version, the handset network address, and/or the like. Roose '556 at 22:15–63 As described in the overview example, location information allows system 100 to authenticate and restrict a user based on the location of the device used by the user to access the network. The location information can be added as an authentication attribute to typical authentication systems. Entry into and usage of a network is typically regulated using authentication systems such as Network Operating Systems (NOSs), Remote Authentication Dial-In User Service (RADIUS), described in IETF Request For Comment (RFC) 2138, and IEEE 802.1X standard, which provides for port-based network access control based on a MAC identifier. In the case of NOS and RADIUS, an authentication server (e.g., 142 (FIG. 8)) provides the mechanism for establishing such authentication. In the case of IEEE 802.1X, the network entry devices 114 may be configured with such authentication capability, as described more fully in that standard. IEEE 802.1Q standard provides another means for controlling access and usage of a network. That standard is directed to the establishment and operation of VLANs. The IEEE 802.1Q standard defines the configuration of network devices to permit packet reception at a configured port entry module. Firewalls (e.g., 140 (FIG. 8)) also provide a technique for network usage regulation. Firewalls are primarily computer programs designed to analyze packets and, from that analysis, make a determination as to whether packet transmission into or out of the network is permitted. Being location-aware, system 100 is able to combine the association of a device's physical location with any of these network access regulations as an attribute to assess permitted network access. For example, a VLAN policy template distributed to network devices to configure VLANs can be accompanied by a physical location constraint. Roose '556 at 22:64–23:9 In general overview of the authentication process, a user device 104 connects to the network infrastructure

Claims	Prior Art
	101, via a connection point 160. System 100 authenticates the device. System 100 receives the location of the device 104 from the device 104 itself and/or from infrastructure 101. System 100 receives user credentials and authenticates the user. During this authentication, system 100 verifies the location of device 104 employing the techniques described herein. If the user is authenticated and the location is both verified and authenticated for the requested network resources, system 100 proceeds in allowing device 104 to access the requested resources. System 100 can log each of these events for administrative use. Roose '556 at 23:40–59 In more detail, FIG. 4 illustrates an example process 401 that system 100 employs to determine whether any restrictions to access the network, based on location, are applicable. Specifically, in example location identification process 401 represented by FIG. 4, a user seeking access to system 100 can be first authenticated (step 405) or otherwise filtered by system 100. System 100 achieves this portion of the authorization process by requiring the end user at a location client device to supply certain user information including but not limited to, a name and one or more passwords (e.g., necessary user credentials). If the user is permitted access to system 100 on that basis (e.g., user name and password), system 100 permits the user to query (step 410) system 100 for access to certain information, applications, and the like. Alternatively or in addition, system 100 receives (step 415) the device location before allowing the requested access. A trusted user device (e.g., 104), a network infrastructure device (e.g., a network entry device 114) and/or a location server can supply the user device location using the techniques as described herein. Roose '556 at 25:34–58 FIG. 5 represents another example authentication process 500. In the illustrated process 500, system 100 obtains (step 505) the location information for an client device. In this case, system 100 employs only the location of the device in determining the appropriate level of service. In another example, system 100 can also employ the user credentials (e.g., user name and password), in addition to the location, to determine the appropriate level of service. System 100 determines (step 510) whether the obtained location is verified. If system 100 determines (step 510) that the location is not verified, system 100 denies (step 515) access or restricts (step 515) access according to predefined policies (e.g., deny any access or restrict access to only those devices, applications and data available to the general public regardless of location). If system 100 determines (step 510) that the location is verified, system 100 determines (step 520) whether the location is authenticated. If system 100 determines (step 520) that the location is not authenticated, system 100 determines (step 525) whether to accept the asserted location. If system 100 determines (step 525) to not accept the asserted location, system 100 denies/restricts (step 515) access

Claims	Prior Art
	according to predefined policies. If system 100 determines (step 525) to accept the asserted location, system 100 allows (step 530) access at selectable service levels, as described below, according to predefined policies. Roese '556 at 26:29–46 Use of the above techniques enables system 100 to restrict access to data, applications, specific networked devices, data and network service, QOS (Quality of Service) levels, network tools, functionality, rules, and the like, based on the user and/or the location of the device associated with the user seeking access. Further to the techniques above, system 100 can employ the location information to effect a modification of the access requirements. For example, when a device seeks network access from a location deemed not to be inherently secure (e.g., such as a public facility like an airport), system 100 can prompt a user to initiate an improved connection, such as a virtual private network (VPN), or can inform the user that supplemental restrictions apply while in the insecure area. More generally, this can be seen as an expansion of policy-based access in that the access rules for an individual user may be adapted as a function of the client device location and/or the level of trust associated with the location information. Roese '556 at 27:29–51 In addition to access control, system 100 can use location information to enforce restrictions regarding the transmission of data. As described in the overview example, location information allows system 100 to deny access to certain sensitive information upon request from a location client outside of a specified region, or to prohibit data from being transmitted through an intermediate device that is located outside of a specified region. FIG. 6 illustrates an example process 601 that system 100 employs to effect these data transmission restrictions. Specifically, in the example information tagging process 601 represented by FIG. 6, system 100 receives (step 605) a request from an end user for access to information (e.g., file, document, and/or the like, generally, data). This assumes that the end user has been adequately authenticated or otherwise permitted access to the network, as described above. System 100 then determines (step 610) whether the requested data is location sensitive. That is, whether the data should not be moved beyond certain defined boundaries (e.g., a present device, a room, a building, a campus, a city, a country and the like). If system 100 determines (step 610) that the data is not location sensitive, system 100 permits (step 615) access to that data that is not restricted by location. Roese '556 at 28:39–57 With a location-aware infrastructure, system 100 can employ trusted location information to provide other services in addition to those described above. For example, system 100 can use the location information in

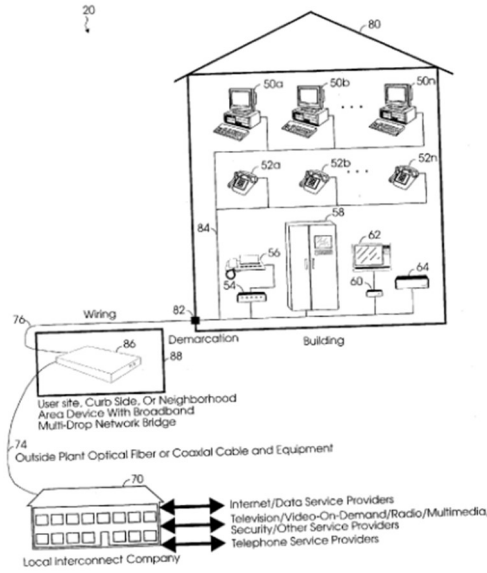
Claims	Prior Art
	emergency situations, where a device may be an alarm or sensor. System 100 determines the location of the alarm device and transmits the location information to a party responding to the alarm. System 100 can also use location information to recover a stolen user device 104. As the stolen user device 104 accesses system 100, system 100 determines the location of the stolen device and transmits the location information to a party seeking to locate the device. System 100 can track mobile user devices (e.g., 104b) and thus can also track anything associated with that user device (e.g., the user, a file, a physical object, and the like). System 100, through the use of location information, can provide these and other services and applications. The examples that follow illustrate how system 100 can employ location information to provide these and other services and applications. Roose '556 at 30:32–45 Referring to FIG. 8, system 100' provides another example of a location-aware network and is described as an enterprise network that serves as a data communications network for a business organization or other type of enterprise. The enterprise operates the network according to various policies, which may include location-dependent aspects. For example, access-control policies may depend on the locations of devices accessing services on the network. In various configurations, system 100' may include or make use of one or more LANs, MANs, WANs, PANs and/or Ethernet to the first mile (e.g., IEEE 802.3ah). In other examples of such a network, the physical and logical arrangement of the devices can differ from that shown in FIGS. 1 and 8. Mandke 2003A at 11 Interference susceptibility refers to the impact that other co-located intentional and unintentional radiators may have on the alt-PHY. The error rate criterion is the maximum packet error rate (PER). Mandke 2003A at 11 The PER should be less than 8% for a 1024 byte packet length when an interferer is present at a separation of 1m from the receiver. A broad representative set of interferers such as WLANs (2.4 GHz and 5 GHz), other WPANs (such as 802.15.1, 802.15.3, and 802.15.4), ISM cordless phones (2.4 GHz and 5 GHz), and radiators such as microwave ovens are the primary cases considered. Mandke 2003A at 11–12 Coexistence refers to the co-location of IEEE P802.15.3a devices with other, non-802.15.3a devices. The 802.15.3a devices must coexist with other receivers such as Bluetooth™ (IEEE 802.15.1), 802.15.3, IEEE

Claims	Prior Art
	802.11b, IEEE 802.11a, and IEEE 802.15.4 that operate in the unlicensed spectrum and which may be co-located with 802.15.3a devices. The minimum criteria here is that the interfering average power generated by the 802.15.3a transmitter and measured in the relevant bandwidth of the victim receiver should be at least 6 dB below the minimum sensitivity level of the non-802.15.3a device operating in the 6 Mbps mode, when the separation between the 802.15.3a transmitter and victim receiver is 1 m. Mandke 2003A at 13 The signal acquisition methods are the techniques by which the proposed receiver acquires and tracks the incoming signal in order to correctly receive the transmitted data. Target acquisition times are less than 6 μs for piconet clear channel assessment (CCA) (referenced to the beginning of the preamble), and less than 20μs for acquisition from the beginning of the preamble to the beginning of the header. Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one radio to another via an intermediate repeater link. Aiello '273 at [0040] Decentralized network 100 also allows uncontrolled deployment of devices, automatic topology management of devices, overlapping network, fair access to burst and priority traffic, and QoS support. Unlike a centralized network, decentralized network 100 does not require a master device to act as a scheduler for traffic.

Claims	Prior Art
	Malan '698 at Abstract A method and system are provided for protecting publicly accessible network computer services from undesirable network traffic in real-time. The method includes receiving network traffic destined for the services and analyzing the network traffic to identify an undesirable user of the services. Access of the undesirable user to the services is limited to protect the services. The method and system identify and remove a new level of security threat that is not addressable by current techniques. Specifically, the method and system identify topologically anomalous application-level patterns of traffic and remove these data flows in real-time from the network. Malan '698 at [0022] An object of the present invention is to provide a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time. Malan '698 at [0023] In carrying out the above objects and other objects of the present invention, a method for protecting publicly accessible network computer services from undesirable network traffic in real-time is provided. The method includes receiving network traffic destined for the services, and analyzing the network traffic to identify an undesirable user of the services. The method further includes limiting access of the undesirable user to the services to protect the services. Malan '698 at [0051] In general, the present invention provides a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time and is useful within a larger system which combats denial of service attacks without requiring any changes to the existing Internet routing infrastructure. This larger system, in general, combines network topology information and coarse-grained traffic statistics from routers to detect, backtrack, and filter distributed attacks on enterprise networks and websites. This larger system exploits information from routers without requiring any changes to the existing Internet routing infrastructure. The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and enterprise networks. The method and system is enabled by functionality that the major routing vendors have put into their latest products.

Claims	Prior Art
	Malan '698 at [0063] FIG. 1 shows an example use of the DoS scrubber. It depicts a network server providing a publicly accessible service—a public Web server for example. The DoS scrubber is interposed between the server and the Internet. As such, it sees all the traffic that passes between the server and its remote clients. As a public server, both legitimate and malicious users gave equal access to its resources. However, by analyzing the service request distributions and packet statistics, the DoS scrubber can identify malicious users of the service and either filter completely or throttle back their access. Malan '698 at [0065] FIG. 2 denotes the denial of service scrubber's high-level architecture. It is comprised of two primary components: the forwarding and the analysis engines. The forwarding engine (FE) has two main responsibilities: applying filtering and rate limiting to sets of Internet hosts, and generating request statistics. The analysis engine (AE) is responsible for the collection and subsequent data mining of the forwarding engine's statistics. Upon detection of malicious hosts, appropriate actions are fed back from the analysis engine to the forwarding engine for filtering or rate limiting the host's requests. Malan '698 at [0066]–[0070] The DoS scrubber's forwarding engine serves both as an enforcement mechanism and statistics generator. When Internet Protocol (IP) packets enter the scrubber, they are given to the forwarding engine. Upon receipt, the FE determines if the packets belong to an old request, or are part of a new request. If the request is new, a variety of safeguards remove many of the common types of denial of service—such as TCP SYN floods. However, the safeguards also include checking to see if requesting client has been determined malicious by the analysis engine. If so, the request is dealt with in a policy configured manner. For example, if the service is not overwhelmed, it may allow the request to happen; however it can be throttled back using a custom rate limiter. When packets arrive that are not discarded, statistics are collected that are later sent to the analysis engine. Examples of these statistics include: Size: the request and subsequent reply's size, both in bytes and packets. Request payload: content of the request at the application layer (e.g., HTTP GET string). Number of fragments: the number of fragments in the request can be used to detect some types of malicious use. Number of protocol anomalies: the number of errors in the request's protocols. Mandke 2003B at 24 The IEEE 802.15.3 task group is developing WPANs up to 55 Mbps. The draft standard operates on five 15 MHz channels in the 2.4 GHz ISM band, two of which interfere with IEEE 802.11b traffic. Modulation

Claims	Prior Art
	(QPSK, DQPSK, 16/32/64-QAM) and coding (trellis-coded modulation) are varied to provide five data rates (11 Mbps, 22 Mbps, 33 Mbps, 44 Mbps, and 55 Mbps) [5]. The MAC layer described by this standard allows for the coordination of WPAN devices to form piconets. The MAC layer also allows for multimedia quality of service (QoS), power management, and ad-hoc networking support. IEEE 802.15.3 gained sponsor ballot approval in May 2003. The focus of UWB occurs in a separate task group, IEEE 802.15.3.a, which is discussed below. Zuk '399 at Abstract Systems and methods for detecting and preventing network security breaches are described. The systems and methods present a gateway-based packet-forwarding network security solution to not only detect security breaches but also prevent them by directly dropping suspicious packets and connections. The systems and methods employ multiple techniques to detect and prevent network security breaches, including stateful signature detection, traffic signature detection, and protocol anomaly detection. Zuk '399 at [0001] This invention relates generally to network security systems and methods for detecting and preventing security breaches on a network. More specifically, the present invention provides gateway-based packet-forwarding network security systems and methods to not only detect security breaches on the network but also prevent them by directly dropping suspicious packets and connections. These systems and methods employ multiple techniques to detect and prevent intrusions, including stateful signature detection, traffic signature detection, and protocol anomaly detection. Melick '146 at 8:11–16 According to one aspect of the present invention, the present invention provides for storing data by persistently maintaining the data on a network, through retransmission. The data can be associated with expiration properties. The expiration properties can include geographical information and/or time attributes. The data can be in packets or streams.
11. The broadband wireless repeater or relay of claim 1, wherein said at least one receiver or transceiver for receiving signals or data and said at least one	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art

Claims	Prior Art
transmitter or transceiver for transmitting signals or data operate in half duplex.	would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 1, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Bareis ’373 at FIG. 2  FIG. 2 Mandke 2003A at 11 Some of the applications IEEE 802.15.3a anticipates supporting are: Voice over IP, HDTV, Home Theater, digital imaging, and location awareness. In March 2003, Task Group 802.15.3a heard the first round of presentations out of the 29 respondents to the CFP (Appendix B) for higher data rate physical layer alternatives to the physical layer in the 802.15.3 standard (55 Mbps in the 2.4 GHz ISM band). The standard being developed by IEEE 802.15.3a will replace the physical layer for IEEE 802.15.3 (i.e. it will use the same media-access control layer as the IEEE 802.15.3 standard). The IEEE is expected to publish

Claims	Prior Art
	the approved standard in mid-2004. Fontana at 2 UWB APPLICATIONS Figure 1 illustrates an ultra wideband, handheld transceiver that was designed for full duplex voice and data transmission at rates of up to 128 kb/s (CVSD) and 115.2 kb/s (RS232). The radio has an operational center frequency in L-band (1.5 GHz) with an instantaneous bandwidth of 400 MHz (27% fractional BW). Peak power output from the UWB transceiver was measured at 2.0 Watts, with a resultant average power (worst case) of 640 μW. This results in a worst case power density of 1.6 pW/Hz. These units have a range of approximately 1 to 2 km (with small antennas shown and line-of-sight), and an extended range of 10 to 20 miles with small gain antennas. Fontana at Figure 1  Figure 1. Full Duplex UWB Handheld Transceivers. Fontana at 3 Figure 3 illustrates a high-speed (up to 25 Mb/s) UWB radio designed for transmission of compressed video and command & control information across an asymmetric, bi-directional link. This system was also designed to operate in the 1.3 to 1.7 GHz region (27% fractional BW) with a 4W peak power output. An earlier design, developed under funding from the U.S. Defense Advanced research Projects Agency (DARPA), operated with a 500 MHz instantaneous bandwidth in the C-band region (5.4 to 5.9 GHz). Fontana at 5 Figure 6 illustrates a set of prototype UWB transceivers designed for the U.S. Navy to provide a wireless intercom capability on-board Navy aircraft. The prototype UWB transceivers provide multichannel, full duplex, 32 kb/s digital voice over a range of approximately 100 meters. An ultra wideband waveform was selected because of its ability to operate in severe multipath (created by multiple RF reflections inside and

Claims	Prior Art
	around aircraft), and because of its non-interfering, low probability of intercept signature.
17. The broadband wireless repeater or relay of claim 1, wherein said repeater or relay employs MIMO or adaptive antenna technology.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said repeater or relay employs MIMO or adaptive antenna technology.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said repeater or relay employs MIMO or adaptive antenna technology” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 1, wherein said repeater or relay employs MIMO or adaptive antenna technology” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. Engels ’850 at 6:29–31 Variable direction antenna is an antenna in which the direction of maximum gain can be changed during operation. An adaptive antenna is a form of variable direction antenna. Engels ’850 at 9:16–26 Generally the second antenna means (10) of the indoor to outdoor coupling unit can be a) an omnidirectional antenna (10, Fig. 6a), b) a directive antenna (10) having a 3dB bandwidth over a limited angle in the azimuth plane, e.g. a half-sphere, and directed towards the outside of the building (Fig. 6b), or c) a directional antenna (10) having a 3dB bandwidth angle less than 180°, e.g. 60° or 90°, pointed to the outdoor antenna (Fig. 6c). In the latter case, due to the larger antenna gain, a higher signal attenuation can be accommodated and the length of the transmission path (6) can be larger. However, such a directional antenna needs usually to be pointed towards the outdoor antenna (9), e.g. manually. Alternatively, the second antenna means may be replaced by connection (30) to a cable network such as an optical fibre cable, a coax cable, a twisted pair cable or similar (Fig. 6d). Engels ’850 at 13:11–16 In another aspect of the invention the usage of multiple antenna techniques with antenna means (10) may result in a communication with antenna's at multiple outdoor nodes located at different locations. This feature is particularly useful for providing redundancy in the outdoor connection. Multiple antenna techniques include beamforming, spatial division multiple access (SDMA), multiple input multiple output

Claims	Prior Art
	(MIMO) systems. Chabas '657 at [0007] The inventive idea thus comprises the use of the teaching given by the architecture known by the name of "MIMO" which proposes to multiply the number of transceiver devices for each secondary station. The idea also comprises to benefit from the system to further improve the MIMO technique by adding transmission paths, by varying the diversity even more. This architecture is described in articles such as, for example: "Capacity results on frequency-selective Rayleigh MIMO channels" by Daniel Pérez et al., published in the Conf. IST-Ireland in October 2000 on pp. 491 to 496. Chabas '657 at [0013] FIG. 2 shows in more detail the structure of the secondary station. According to the invention the secondary station 23 is in essence constituted by a plurality of receiving devices RX1 to RXm and a plurality of transmitting devices TX1 to TXn. The various receiving devices RX1 to RXm supply their information to a processing circuit 40 to establish useful information at a receiving access 42 to be used. In a similar manner, useful information to be transmitted, available on a transmit access 50 is distributed by means of a transmission processing circuit 52 to various transmitting devices TX1 to TXn. The number of transmission devices may be equal to the number of receiving devices ($m=n$). This secondary station thus has a structure of a type known by the name of MIMO cited above. These transmitting devices and these receiving devices may have radio traffic with the sole station 21. But it is also possible that a certain number of these transmitting devices have radio traffic with the base station, whereas the others have radio traffic with the secondary station 21. This is shown in the Figure by arrows FT and FR, which indicate the transmission and reception, respectively, for the station 23. It will be recalled that the function of relay or repeater effected by the station 21 permits a better processing, for the diversity is ensured in this case at the level of the station 23. Chabas '657 at [0014]–[0017] By the invention: the concept of the MIMO architecture is extended to the repeater mode of the operation in a cellular network and in a more particular manner for the ODMA mode and for FDD (Frequency Division Diversity), a contribution is made towards further reduction of the noise level in the small cells for which the ODMA mode is implemented and as a result of which the quality of the services offered by the network and the capacity of traffic of the cell is improved,

Claims	Prior Art
	a contribution is also made towards improving the transition process between these modes. There is a parallel processing of the transmitted data, which permits to go to the TDD mode (Time Division Diversity) as this is done in the FDD mode. Gardner '709 at Abstract A modified preamble is used by extended devices that operate at higher rates, MIMO or other extensions relative to strict 802.11a-compliant devices. The extended devices might use multiple antenna techniques (MIMO), where multiple data streams are multiplexed spatially and/or multi-channel techniques, where an extended transmitter transmits using more than one 802.11a channel at a time. Such extensions to IEEE 802.11a can exist in extended devices. The modified preamble is usable for signaling, to legacy devices as well as extended devices, to indicate capabilities and to cause legacy devices or extended devices to defer to other devices such that the common communication channel is not subject to unnecessary interference. The modified preamble. is also usable for obtaining MIMO channel estimates and/or multi-channel estimates. The modified preamble preferably includes properties that facilitate detection of conventional and/or extended modes ("mode detection") and provides some level of coexistence with legacy IEEE 802.11a devices. Gardner '709 at [0008] One approach to obtaining higher data rates is the use of more bandwidth. Another approach, used by itself or as well as the use of more bandwidth, is MIMO (multiple-input, multiple-output) channels, where a plurality of transmitters transmit different data or the same data separated by space to result in possibly different multi-path reflection characteristics. In either case, care is needed for coexistence and interoperability between legacy devices and extended devices. Gardner '709 at [0031] 4) Extended MIMO in multiple 20 MHz channels (e.g., 40, 60, 80, or 100 MHz channels) Gardner '709 at [0049] Some modified preamble structures described herein provide interoperability and coexistence between SISO multi-channel packets/devices and MIMO multi-channel packets/devices, as well as coexistence between multi-channel packets/devices and legacy packets/devices.

Claims	Prior Art																		
26. The broadband wireless repeater or relay of claim 1, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 1, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 1, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [9d].</i>																		
29[pre]. A broadband wireless repeater or relay, comprising:	“A broadband wireless repeater or relay” was well known at the time of the alleged invention. A person of ordinary skill in the art would have found it obvious to modify an existing device to include the claimed elements as set forth below and in Defendants’ other invalidity charts. For example: See, e.g.: <table border="0"> <tr> <td>337-A01</td><td>U.S. Pat. No. 6,584,080 (“Ganz ’080”)</td></tr> <tr> <td>337-A02</td><td>U.S. Pat. Pub. No. 2002/0028655 (“Rosener ’655”)</td></tr> <tr> <td>337-A03</td><td>U.S. Pat. Pub. No. 2004/0160928 (“Perlman ’928”)</td></tr> <tr> <td>337-A04</td><td>U.S. Pat. No. 6,188,496 (“Krishna ’496”)</td></tr> <tr> <td>337-A05</td><td>U.S. Pat. No. 7,209,523 (“Larrick ’523”)</td></tr> <tr> <td>337-A06</td><td>U.S. Pat. No. 4,056,780 (“Faulkner ’780”)</td></tr> <tr> <td>337-A07</td><td>U.S. Pat. No. 6,497,656 (“Evans ’656”)</td></tr> <tr> <td>337-A08</td><td>U.S. Pat. Pub. No. 2003/0120809 (“Bellur ’809”)</td></tr> <tr> <td>337-A09</td><td>U.S. Pat. No. 8,125,940 (“Perlman ’940”)</td></tr> </table>	337-A01	U.S. Pat. No. 6,584,080 (“Ganz ’080”)	337-A02	U.S. Pat. Pub. No. 2002/0028655 (“Rosener ’655”)	337-A03	U.S. Pat. Pub. No. 2004/0160928 (“Perlman ’928”)	337-A04	U.S. Pat. No. 6,188,496 (“Krishna ’496”)	337-A05	U.S. Pat. No. 7,209,523 (“Larrick ’523”)	337-A06	U.S. Pat. No. 4,056,780 (“Faulkner ’780”)	337-A07	U.S. Pat. No. 6,497,656 (“Evans ’656”)	337-A08	U.S. Pat. Pub. No. 2003/0120809 (“Bellur ’809”)	337-A09	U.S. Pat. No. 8,125,940 (“Perlman ’940”)
337-A01	U.S. Pat. No. 6,584,080 (“Ganz ’080”)																		
337-A02	U.S. Pat. Pub. No. 2002/0028655 (“Rosener ’655”)																		
337-A03	U.S. Pat. Pub. No. 2004/0160928 (“Perlman ’928”)																		
337-A04	U.S. Pat. No. 6,188,496 (“Krishna ’496”)																		
337-A05	U.S. Pat. No. 7,209,523 (“Larrick ’523”)																		
337-A06	U.S. Pat. No. 4,056,780 (“Faulkner ’780”)																		
337-A07	U.S. Pat. No. 6,497,656 (“Evans ’656”)																		
337-A08	U.S. Pat. Pub. No. 2003/0120809 (“Bellur ’809”)																		
337-A09	U.S. Pat. No. 8,125,940 (“Perlman ’940”)																		

Claims	Prior Art
	337-A10 U.S. Pat. Pub. No. 2005/0201326 (“Lakkis ’326”) 337-A11 U.S. Pat. Pub. No. 2004/0048574 (“Walker ’574”) 337-A12 XtremeSpectrum Trinity Chipset <i>See above at row 1[pre].</i>
[29a] at least one receiver or transceiver for signal or data reception from one or more devices;	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “at least one receiver or transceiver for signal or data reception from one or more devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “at least one receiver or transceiver for signal or data reception from one or more devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “at least one receiver or transceiver for signal or data reception from one or more devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1a].</i>
[29b] at least one transmitter or transceiver for signal or data transmission to one or more devices,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “at least one transmitter or transceiver for signal or data transmission to one or more devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “at least one transmitter or transceiver for signal or data transmission to one or more devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “at least one transmitter or transceiver for signal or data transmission to one or more devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1a].</i>
[29c] wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different; and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include

Claims	Prior Art
	“wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein the transceiver for signal or data reception and the transceiver for signal or data transmission may be the same or different” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1c].</i>
[29d] a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “a controller that is configured or configurable for operation in one or more wireless networks, said controller communicating with said at least one receiver or transceiver for signal or data reception and said at least one transmitter or transceiver for signal or data transmission” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1d].</i>
[29e] wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100 Megabits per second or more.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or

Claims	Prior Art
have a data transmission rate of 100 Megabits per second or more,	have a data transmission rate of 100 Megabits per second or more” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein at least one of said receiver or transceiver for signal or data reception and said transmitter or transceiver for signal or data transmission either or both transmit and receive at an instantaneous or overall occupied bandwidth of 100 MHz or more or have a data transmission rate of 100 Megabits per second or more” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1e].</i>
[29f] wherein said repeater or relay employs MIMO or adaptive antenna technology,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said repeater or relay employs MIMO or adaptive antenna technology.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said repeater or relay employs MIMO or adaptive antenna technology” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said repeater or relay employs MIMO or adaptive antenna technology” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 17.</i>
[29g] wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices, and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said broadband wireless repeater or relay is used to support connectivity and/or position location capabilities for one or more mobile or portable devices” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1g].</i>

Claims	Prior Art
[29h] wherein said controller is configured or configurable to perform or for performing at least one of:	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “wherein said controller is configured or configurable to perform or for performing at least one of.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “wherein said controller is configured or configurable to perform or for performing at least one of” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “wherein said controller is configured or configurable to perform or for performing at least one of” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1d].</i>
[29i] a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources; and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “a) ignore or filter out at least some signal or data transmissions from one or more undesired transmitters, users, networks, data sources, or noise sources” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [1h].</i> Fontana at 3 As in the above example, this radio was capable of both digital voice and data transmission to 128 kb/s and had an operational range over water of approximately 10 miles using a standard SINCGARS (30-88 MHz) VHF military antenna. Operational range over land depended upon terrain, but was observed to be from 1 to 5 miles with intervening foliage, buildings and hills. [Note that multipath cancellation is a serious problem over water, even with UWB impulse technology, because of the typically low grazing angles (resulting in small differential delays between direct and reflected paths) and strong, out-of-phase reflection from the water surface. Thus, both higher frequency UWB systems as well as more conventional narrowband VHF/UHF radios were unable to provide the requisite performance.] Also unique to the receiver design was the addition of anti-jam circuitry to prevent loss of sensitivity due to

Claims	Prior Art
	strong, in-band interferers commonly observed in this frequency range. The units could also be operated in a "digipeater" mode in which packet store-and-forward techniques were used to transmit data from one radio to another via an intermediate repeater link. Malan '698 at Abstract A method and system are provided for protecting publicly accessible network computer services from undesirable network traffic in real-time. The method includes receiving network traffic destined for the services and analyzing the network traffic to identify an undesirable user of the services. Access of the undesirable user to the services is limited to protect the services. The method and system identify and remove a new level of security threat that is not addressable by current techniques. Specifically, the method and system identify topologically anomalous application-level patterns of traffic and remove these data flows in real-time from the network. Malan '698 at [0022] An object of the present invention is to provide a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time. Malan '698 at [0023] In carrying out the above objects and other objects of the present invention, a method for protecting publicly accessible network computer services from undesirable network traffic in real-time is provided. The method includes receiving network traffic destined for the services, and analyzing the network traffic to identify an undesirable user of the services. The method further includes limiting access of the undesirable user to the services to protect the services. Malan '698 at [0051] In general, the present invention provides a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time and is useful within a larger system which combats denial of service attacks without requiring any changes to the existing Internet routing infrastructure. This larger system, in general, combines network topology information and coarse-grained traffic statistics from routers to detect, backtrack, and filter distributed attacks on enterprise networks and websites. This larger system exploits information from routers without requiring any changes to the existing Internet routing infrastructure. The larger system as well as the present invention works with the existing routing infrastructure deployed at Internet service providers, application service providers, and

Claims	Prior Art
	enterprise networks. The method and system is enabled by functionality that the major routing vendors have put into their latest products. Zuk '399 at [0052] Intruding packets are detected and prevented from spreading to the private or outside networks by the protocol anomaly detection, stateful signature detection, and traffic signature detection software modules. Intruding packets are those containing network attack identifiers associated with network security breaches. Such network attack identifiers may be protocol irregularities, attack signatures, traffic signatures, or a combination of one or more of these, among others. The protocol anomaly detection module looks at the packet flows arranged by the flow manager software module to determine irregularities in the network protocol specifications in the packet. The stateful signature detection module matches known attack signatures to the TCP data stream in case of TCP packets and to the headers and data of packets transmitted with other network protocols. The traffic signature module matches traffic signatures to the network traffic to detect attacks such as port scans and network sweeps. Incoming packets that are judged malicious are dropped by the sensor before reaching any of the network hosts and likewise, outgoing packets are dropped by the sensor before reaching the outside network. The sensor may also drop all the packets in a given session if one or more of its packets are considered to be malicious.
[29j] b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “b) instruct one or more devices or networks to ignore or disregard at least some signal or data transmissions of one or more undesired transmitters, undesired users, undesired networks, or noise sources” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [29i].</i>

Claims	Prior Art
30. The broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform a).	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform a).” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform a)” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform a)” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 6.</i>
32. The broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform network provisioning or monitoring.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform network provisioning or monitoring.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform network provisioning or monitoring” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 29, wherein said controller is configured or configurable to perform network provisioning or monitoring” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
33[pre]. The broadband wireless repeater or relay of claim 32, wherein the network provisioning or monitoring includes one or more of:	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[claim limitation].” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[claim limitation]” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[claim limitation]” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 1[pre].</i>

Claims	Prior Art
[33a] i) bandwidth or delay provisioning of repeated or relayed transmissions,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “i) bandwidth or delay provisioning of repeated or relayed transmissions.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “i) bandwidth or delay provisioning of repeated or relayed transmissions” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “i) bandwidth or delay provisioning of repeated or relayed transmissions” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
[33b] ii) application prioritization,	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “ii) application prioritization.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “ii) application prioritization” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “ii) application prioritization” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>
[33c] iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth, and	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “iii) prioritizing, delaying or altering of data transmissions, traffic, or bandwidth” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 8.</i>

Claims	Prior Art
[33d] iv) monitoring or measuring traffic from one or more devices, users or networks.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “iv) monitoring or measuring traffic from one or more devices, users or networks.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “iv) monitoring or measuring traffic from one or more devices, users or networks” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “iv) monitoring or measuring traffic from one or more devices, users or networks” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [9d].</i>
35. The broadband wireless repeater or relay of claim 29, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex.	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 29, wherein said at least one receiver or transceiver for receiving signals or data and said at least one transmitter or transceiver for transmitting signals or data operate in half duplex” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row 11.</i>
48. The broadband wireless repeater or relay of claim 29, wherein one or more of said receiver or transceiver for signal or data reception, said transmitter or transceiver for signal or data transmission, and said controller is	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein one or more of said receiver or transceiver for signal or data reception, said transmitter or transceiver for signal or data transmission, and said controller is embedded in one or more integrated circuit chips.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein one or more of said receiver or transceiver for signal or data reception, said transmitter or transceiver for signal or data

Claims	Prior Art
embedded in one or more integrated circuit chips.	transmission, and said controller is embedded in one or more integrated circuit chips” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 29, wherein one or more of said receiver or transceiver for signal or data reception, said transmitter or transceiver for signal or data transmission, and said controller is embedded in one or more integrated circuit chips” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at claim 1.</i> Mandke 2003B at 23 The key to UWB will be the development of low power CMOS chip technology up to the 10 GHz band, which many manufacturers are presently perfecting. Spectrum regulators in other countries have yet to authorize UWB, and are waiting to see how UWB performs in the U.S. In fact, the standards activity in the U.S. is being developed to anticipate varying spectral allocations in other countries. Discrete Time Proposal at Slide 3 Goals • Good use of UWB unlicensed spectrum • Good system design • Path to low complexity CMOS design • Scalable to future standards • Graceful co-existence with other services
49. The broadband wireless repeater or relay of claim 29, wherein said broadband wireless	It was well known and routine at the time of the alleged invention for a broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or

Claims	Prior Art
repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay.	transmitted by said broadband wireless repeater or relay.” To the extent a broadband wireless repeater or relay disclosed in any of Defendants’ other invalidity charts is found not to disclose this limitation, a person of ordinary skill in the art would have found it obvious to modify an existing broadband wireless repeater or relay to include “[t]he broadband wireless repeater or relay of claim 29, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay” as claimed in light of the teachings in the references set forth below and in Defendants’ other invalidity charts. These prior art references further demonstrate that the claimed “[t]he broadband wireless repeater or relay of claim 29, wherein said broadband wireless repeater or relay is configured or configurable for monitoring or measuring traffic passed through, received by or transmitted by said broadband wireless repeater or relay” would have been incorporated into a broadband wireless repeater or relay with reasonable expectation of success. <i>See above at row [9d].</i>