US 20040203870A1

(19) **United States**

(12) **Patent Application Publication**

Aljadeff et al.

(10) **Pub. No.: US 2004/0203870 A1**

(43) **Pub. Date: Oct. 14, 2004**

(54) **METHOD AND SYSTEM FOR LOCATION FINDING IN A WIRELESS LOCAL AREA NETWORK**

(76) Inventors: **Daniel Aljadeff**, Kiriat Ono (IL); **Yair Granot**, Modlin (IL); **Shalom Tsruya**, Rishon Lezion (IL)

Correspondence Address:
WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251 (US)

(21) Appl. No.: **10/225,267**

(22) Filed: **Aug. 20, 2002**

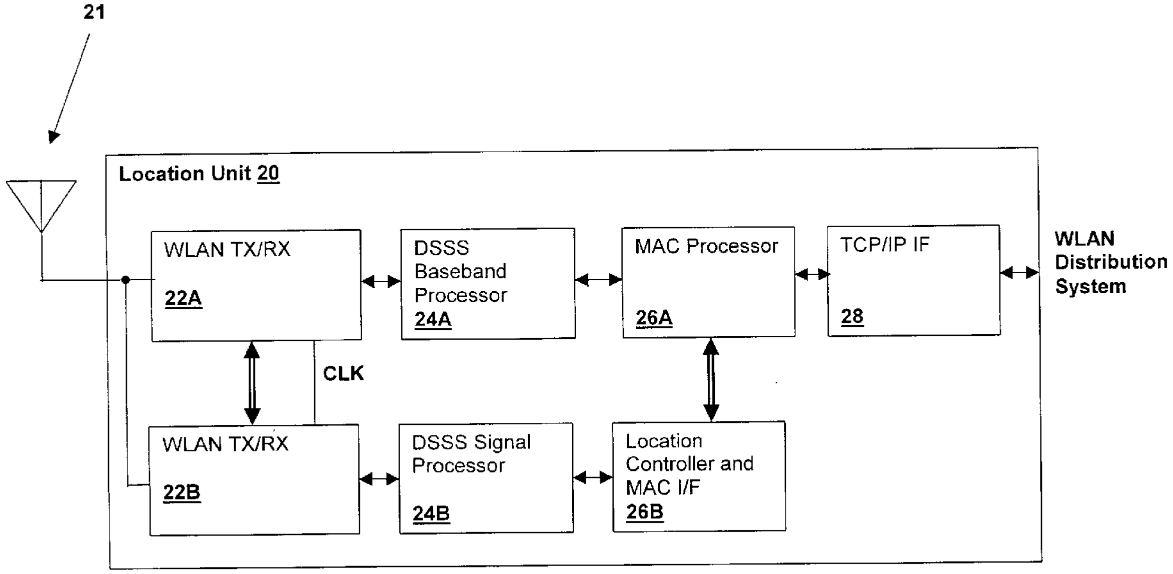
Publication Classification

(51) **Int. Cl.**^{7} **H04Q 7/20**

(52) **U.S. Cl.** **455/456.1**; 455/457

(57) **ABSTRACT**

A method and system for location finding in a wireless local area network (LAN) enables enhanced security via network intrusion management and connection access management, as well as providing a mechanism for physically mapping a wireless network. Multiple receivers are employed to determine time-difference-of-arrival (TDOA) of signals transmitted from a wireless device. The location of the transmitting device is determined by triangulating between multiple receivers. The receivers may be devices within the wireless network that have been enhanced to include TDOA capability, or multiple dedicated location units may be employed within the wireless network or a wired network that may be a completely separate infrastructure depending on the requirements of a particular installation.



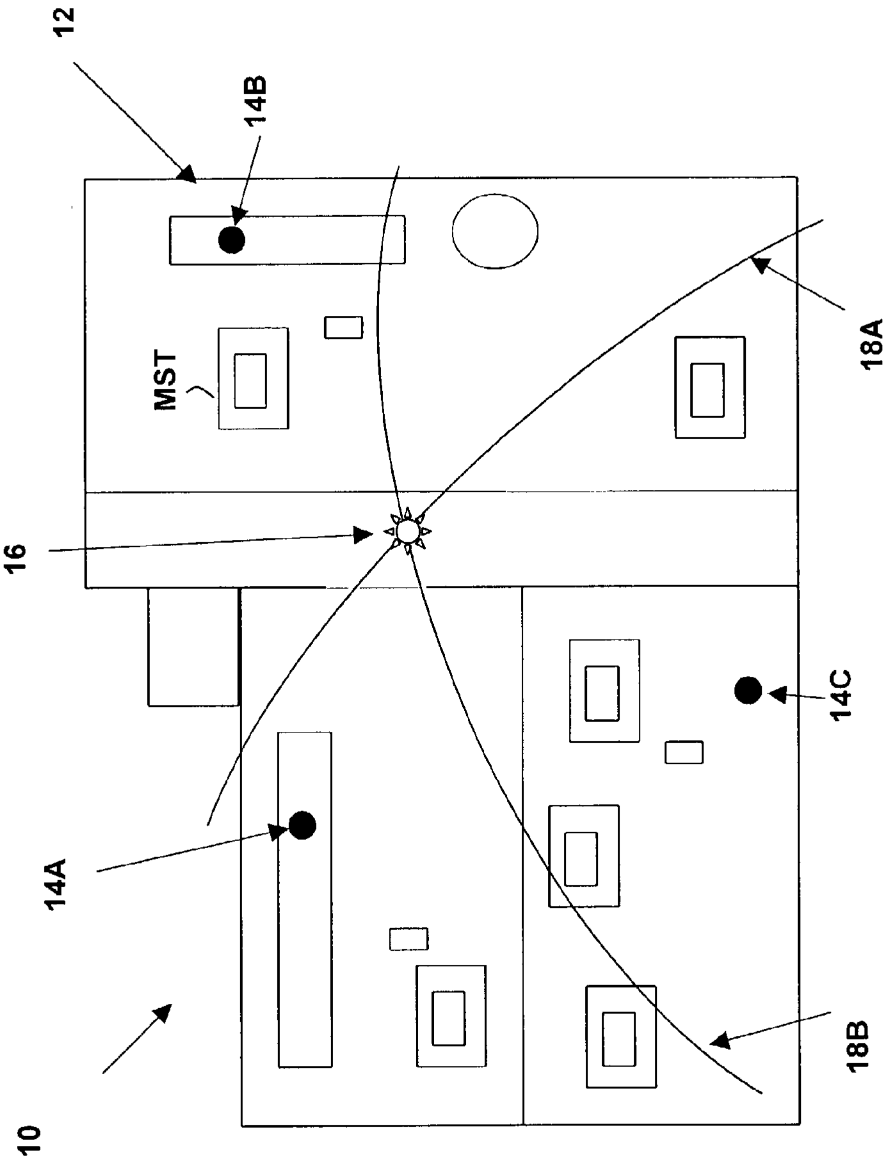


Fig. 1

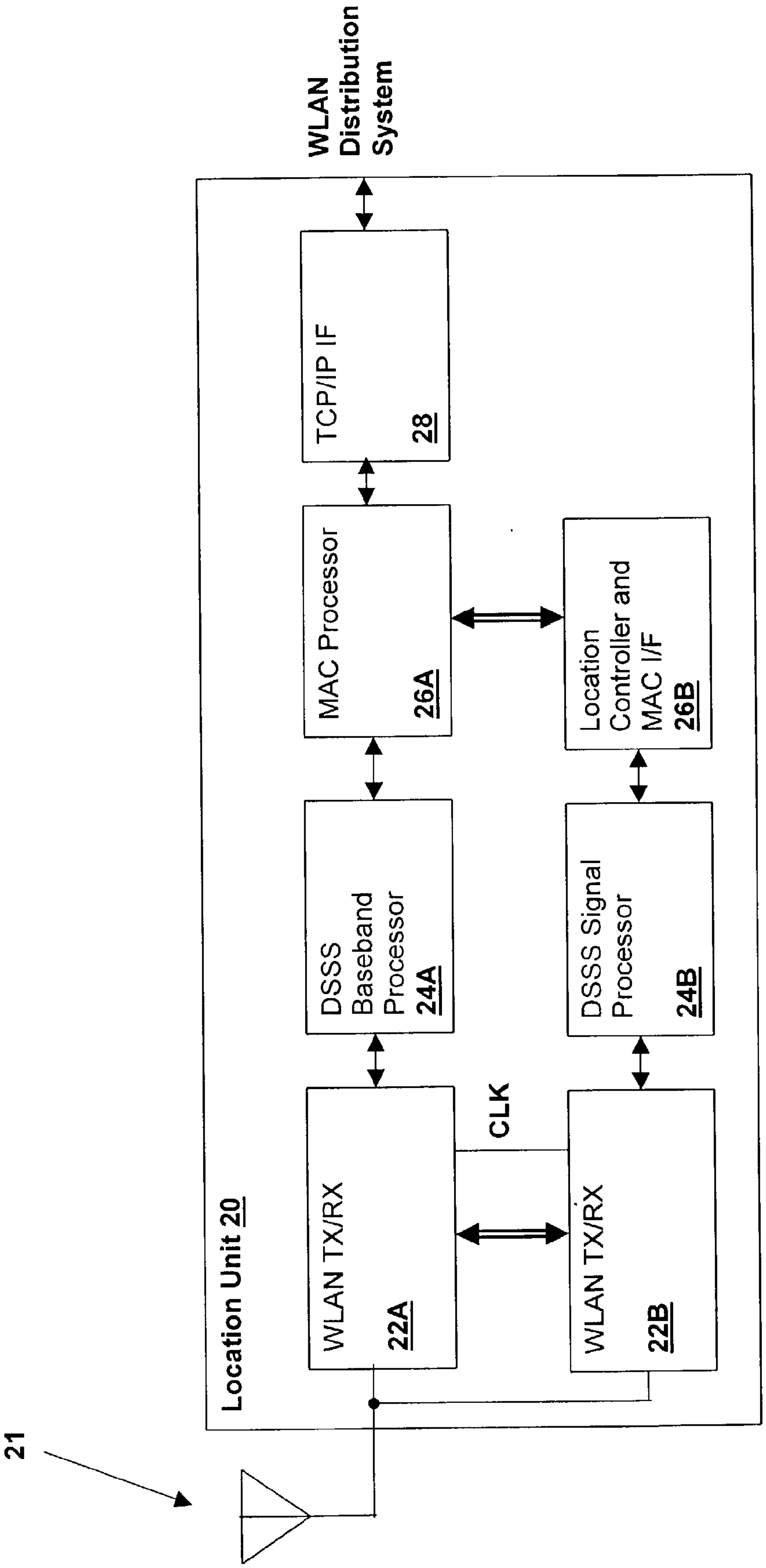

WLAN Distribution System
TCP/IP IF
28
MAC Processor
26A
Location Controller and MAC I/F
26B
DSSS Baseband Processor
24A
DSSS Signal Processor
24B
CLK
WLAN TX/RX
22A
WLAN TX/RX
22B
Location Unit 20
21

Fig. 2

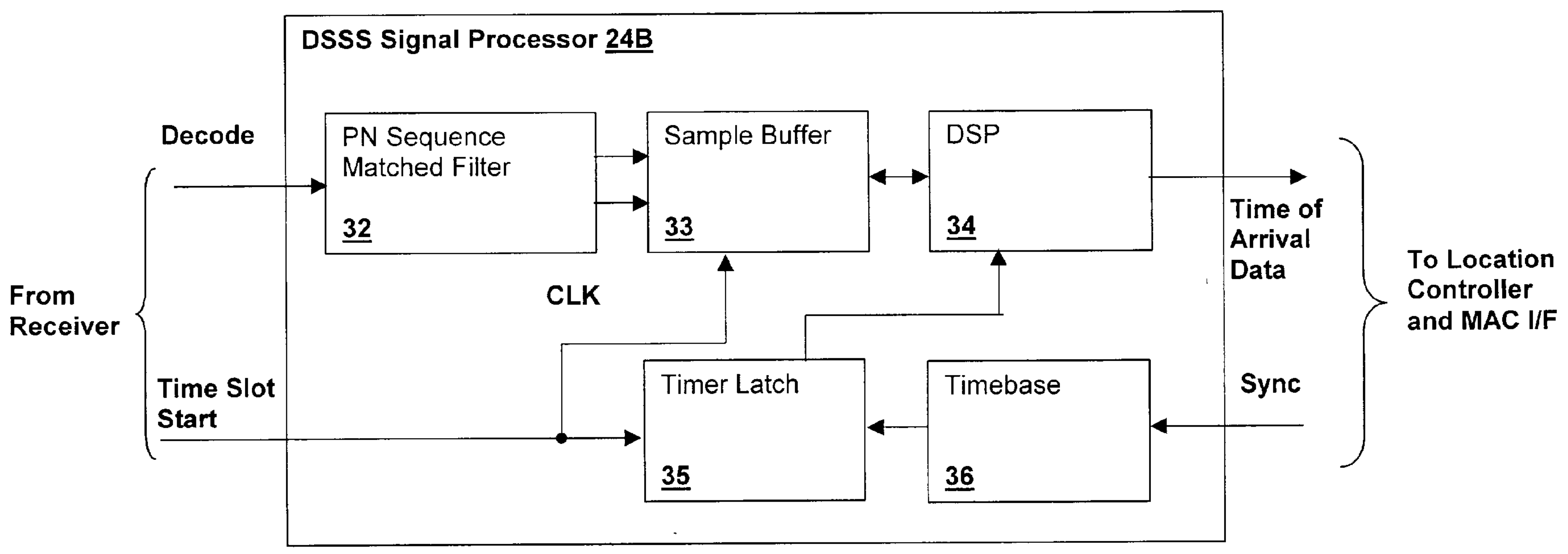

DSSS Signal Processor 24B
Decode
From Receiver
Time Slot Start
PN Sequence Matched Filter
32
Sample Buffer
33
DSP
34
CLK
Timer Latch
35
Timebase
36
Time of Arrival Data
Sync
To Location Controller and MAC I/F

Fig. 3

METHOD AND SYSTEM FOR LOCATION FINDING IN A WIRELESS LOCAL AREA NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is related to previously-filed United States patent applications assigned to the same assignee: "METHOD AND APPARATUS FOR ENHANCING SECURITY IN A WIRELESS NETWORK USING DISTANCE MEASUREMENT TECHNIQUES", Ser. No. 10/156,244, filed May 24, 2002 and "METHOD AND APPARATUS FOR INTRUSION MANAGEMENT IN A WIRELESS NETWORK USING PHYSICAL LOCATION DETERMINATION", Ser. No. 10/171,427, filed Jun. 13, 2002. The specifications of the above-referenced U.S. patent applications are herein incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates generally to wireless networks, and more specifically, to a method and system for determining the physical location of devices within a wireless network.

[0004] 2. Background of the Invention

[0005] A multitude of wireless communications systems are in common use today. Mobile telephones, pagers and wireless-connected computing devices such as personal digital assistants (PDAs) and laptop computers provide portable communications at virtually any locality. Wireless local area networks (WLANs) and wireless personal area networks (WPANs) according to the Institute of Electrical and Electronic Engineers (IEEE) specifications 802.11 (WLAN) (including 802.11a, 802.11b, etc.), 802.15.1 (WPAN) and 802.15.4 (WPAN-LR) also provide wireless interconnection of computing devices and personal communications devices, as well as other devices such as home automation devices.

[0006] Within the above-listed networks and wireless networks in general, it is desirable to know the location of devices for operation of location-based services, mapping of network facilities, and security. The above-incorporated patent applications describe wireless networks in which intrusion management and connection access control use a physical location determination as an indicator of the desirability of a particular connection to a wireless device. It is further desirable to provide services based on the location of a device, such as coupling of a portable device to a workstation when the devices are in proximity, or provision of a financial transaction menu when the portable device is brought in proximity with a transaction terminal.

[0007] Techniques that may be used to determine location are disclosed in the above-incorporated patent applications. The techniques include loop delay measurement for distance determination or received signal strength measurement (RSSI), time-difference-of-arrival techniques (TDOA), and angle-of-arrival techniques (AOA) for location finding. However, the infrastructure of present-day wireless networks has not been adapted to provide physical location determination.

[0008] Existing systems that determine the physical location of assets (that may include wireless network devices) typically use a separate radio-frequency identification (RFID) tag attached to the asset. The RFID tag broadcasts a signal, separate from the wireless network signals and protocols, that can be received at a short distance by a specially adapted receiver.

[0009] The use of tags for locating wireless network devices adds cost and complexity to the wireless network. Also, the tags are typically battery-operated devices that are attached to the asset, and as such have a limited life or will require replacement of the power source. Further, the separate attachment of tags is an inconvenience and is subject to incorrect tagging or tampering such as removal from the asset or relocation to another asset.

[0010] Therefore, it would be desirable to provide a method and system for location finding in a wireless network, so that the physical location of wireless network devices may be determined, and without adding tags or using special signals for determining the location of wireless network devices.

SUMMARY OF THE INVENTION

[0011] The above objectives of physically locating devices in a wireless network is achieved in a method and system. The method is embodied in a system that determines a physical location of a wireless device by comparing the time difference between signals received from the wireless device at multiple receiving stations. The arrival times of the signals are sent from each of the multiple receiving stations to a master unit, where they are compared to known physical location information for the receiving stations stored within the master unit. The master unit then determines the location of the wireless device in conformity with the differences between arrival times at the multiple receiving stations and their known locations. The location of standard wireless network devices having no special location-finding circuitry can be determined by the location units and standard network signaling can be detected and time difference measurements performed thereon to determine the locations of standard network devices.

[0012] The receiving stations may be transceivers, receive only devices or devices performing other network functions that have been enhanced to include embodiments of the present invention. The receiving stations further may be hard-wired to a network channel to provide secure sharing of time difference data, or the time difference data may be communicated via the wireless network channels or via other wireless means. The master device may also be one of the receiving stations.

[0013] The foregoing and other objectives, features, and advantages of the invention will be apparent from the following, more particular, description of the preferred embodiment of the invention, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] **FIG. 1** is a pictorial diagram depicting a wireless network in accordance with an embodiment of the present invention.

[0015] **FIG. 2** is a block diagram of a location finding unit in accordance with an embodiment of the present invention.

[0016] **FIG. 3** is a graph depicting operation of multiple location finding units in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENT

[0017] The present invention provides location finding within a wireless network, such as a WLAN (e.g., IEEE 802.11) or WPAN network, by determining a time-difference-of-arrival (TDOA) profile for signals received from wireless devices connected to or attempting to connect to the wireless network. Once the location of a wireless device is determined via the TDOA profile, location-based services can be provided, the device can be mapped in a network facility map, and security can be managed in conformity with the device's location. In contrast to the use of RFID tags, the present invention provides a wireless network with location-finding capability where no special signaling (e.g., the separate channels used by the RFID tags) and no separate device or tag is required.

[0018] Existing wireless network devices (generally the access points or "APs") may be enhanced to provide a TDOA measurement of physical device location without adding a separate infrastructure, thereby providing position determination and consequent enhanced network security with low incremental cost. Alternatively, a separate infrastructure employing a series of dedicated location finding units may be added to a wireless network facility for providing device location information, avoiding the need to replace installed devices or otherwise reconfigure the wireless network. By adding a set of dedicated location finding units, standard network signals (e.g., request-to-send (RTS), clear-to-send (CTS) and beacon signals (broadcast) can be observed and used to determine the location of the transmitting devices) and standard wireless network devices can be located without requiring any modification to the located devices.

[0019] In TDOA techniques, the location of a transmitting source can be determined by triangulation based on the timing between the signal arrivals at the multiple receivers. Referring now to the figures and in particular to **FIG. 1**, a wireless network **10** within which the present invention is embodied is depicted in a pictorial diagram. Access points (APs) **14**A-**14**C include time-of-arrival (TOA) electronics and software for measuring the arrival time of signals from other wireless network devices. One such device, wireless device **16** is depicted at the intersection of two hyperbolic curves **18**A and **18**B. Curves **18**A and **18**B represent points for which the difference between TOAs for a pair of locating device (APs **14**A and **14**C for curve **18**B and APs **14**B and **14**C for curve **18**A) is a constant. Therefore, once a pair of TOAs are determined by two of APs **14**A-C, a curve may be drawn that intersects the location of the device that transmitted the signal received by the pair of APs. The TOA difference from another pair of APs is then used to determine a second curve and the intersection of the two curves yields the physical location of the transmitting device. The curves are hyperbolic with foci a the location of each of the APs in the pair, since the hyperbolic curve represents the set of points for which the difference between the distance to the two foci is a constant. A particular TOA difference determines the particular curve (i.e., a new curve is generated for each measurement) and represents all of the possible positions of the transmitting device for the determined TOA difference (TDOA) between a pair of receivers. There are two hyperbolic curves that satisfy the absolute value time difference location equation, but the sign of the time difference determines the proper curve, as for negative signs, the hyperbolic curve on which the transmitting device lies is the one closest to the base station for which the time or arrival was subtracted.

[0020] Extending the above-described technique, if at least three receivers are employed, it is possible to locate a transmitting device in two dimensions via the intersection of the two curves generated by two pairs of receivers is detected. The technique can be further extended to three-dimensional space using hyperbolic sections and/or additional pairs of receivers can be used to reduce error in measurement by interpolating between location results or rejecting location results that are bad statistical fits for the measurement.

[0021] The curve calculations described above are performed by a master unit MST (which may be one of the location units or software executing within of another network device) that receives the TOA information from each of the location units (APs **14**A-C in the exemplary embodiment), calculates the differences and determines the location of the transmitting device via the intersection of the above-described hyperbolic curves. Master unit MST may also provide synchronization between the location units (or an independent synchronization mechanism may be employed) and control of the location finding process by requesting that the location units capture TOA information and send the TOA information to master unit MST.

[0022] Generally, the present invention uses wireless network signals that are already in place for network communications and while the system of the present invention may monitor communications without intervening in wireless network operation, active location finding may be performed in accordance with an embodiment of the present invention. A useful protocol is to transmit a request-to-send to a particular wireless network device to be located. The TDOA computations can be performed on the clear-to-send response generated by the particular device. In the above-described manner, the wireless network (or a particular device only) may be polled in order to obtain low-latency location information for a device, the entire network or a portion thereof.

[0023] Referring now to **FIG. 2**, an enhanced wireless network device, in which an embodiment of the present invention is included, is depicted in a block diagram. Location unit **20** may be a dedicated location unit, or may be a wireless network device having enhanced features for location determination according to TDOA measurements. A WLAN transmitter/receiver **22**A is coupled to an antenna **21** for receiving wireless network signals, which will generally be digital spread-spectrum signals (DSSS). A DSSS baseband processor **24**A detects and decodes the DSSS signals and passes the decoded information to a media access control (MAC) processor **26**A that generates MAC (layer **3**) network packets and passes then to a transmission control protocol/Internet protocol (TCP/IP) interface **28** for conversion to the TCP/IP (layer **4**) packets for communication with the network-coupled device. In the return direction, TCP/IP packets received from the network-coupled device at TCP/IP interface **28** are converted to MAC packets by MAC processor **26**A and are passed for encoding (DSSS modulation) to DSSS baseband processor **24**A, which provides a signal input to the transmit portion of WLAN transmitter/receiver **22**A. WLAN transmitter/receiver **22**A transmits a wireless network signal to other network devices via antenna **21**.

[**0024**] A location signal section is provided by a second WLAN transmitter/receiver **22**B (or a single transmitter/receiver can be used for the location section and network section of the location unit as long as the TOA measurement requirements are fulfilled by the receiver design). WLAN transmitter/receiver **22**B receives a signal from antenna **21** and sends it to a special DSSS processor **24**B that determines the TOA of the received signal. The TOA information is passed to a location controller that includes a MAC interface **26**B coupled to MAC processor **26**A in the network section, so that the TOA information can be communicated to a master unit within the wireless network. Alternatively, the communications path from MAC interface **26**B can be passed to a non-wireless Ethernet interface or other wired LAN interface for communicating the TOA information to the master unit.

[**0025**] The signaling components of location unit **20** are depicted as two separate subsystems coupled to the same antenna **21**, but the structure of a wireless network device in accordance with embodiments of the present invention may be varied. For a location-only unit (i.e., a device that provides only the location-finding capability of the present invention without serving as a wireless network access point or other devices) may be implemented by including only the location signal section comprising WLAN transmitter/receiver **22**B coupled to antenna **21** and DSSS processor **24**B. Alternatively a fully network capable wireless device may include all of the depicted elements, but the transmitter/receiver blocks and DSSS processing blocks may be merged as mentioned above with respect to the transmitter/receiver, so that the location finding capabilities of the present invention are integrated within the standard wireless network device electronics. However, while standard signal processing blocks for a wireless network device generally process only the messages encoded for the address of the device (message level detection), location units decode the symbol level of these otherwise undeciphered messages to determine time of arrival information. If the location unit itself is addressed, or the location unit knows the address of another wireless device, message level detection can further enhance the signal to noise ratio of the location finding. The message level detection improves the signal to noise ratio of the location measurement by using known address information to further decode the message, permitting rejection of spurious signals, and raising the confidence of the measurement.

[**0026**] Referring now to **FIG. 3**, details of DSSS processor **24**B are depicted in a block diagram. The decode input accepts signals from a receiver (WLAN transmitter/receiver **22**B) and a PN sequence matched filter **32** correlates the location signal to provides a series of samples in (I,Q) pairs that are stored in a sample buffer **33**. Matched filter **32** provides increased immunity from multipath effects due to reflections within the network facility. Therefore, the locations of access points (or another network device used to perform location measurements) do not need to be optimized to achieve accurate location finding results. If the immunity to multipath effects was lower than that provided by the system of the present invention, the position of the transmitting devices (generally access points being observer) and location units would require careful control of placement in order to avoid location error due to multipath effects. In some multipath environments, it would not be possible to locate all of the devices such that multipath error could be sufficiently reduced.

[**0027**] A Time Slot Start signal is provided by WLAN transmitter/receiver **22**B and is used to start the sampling process via a timer latch **35**. A timebase **36** provides synchronization of the location unit containing DSSS processor **24**B to the other location units, so that the TOA information is precisely related among the locating units and the TDOA differences computed are accurate. A digital signal processor (DSP) **34** computes the TOA of a received signal and transmits the TOA information to the master unit over the wireless network. Location controller and MAC interface **26**B sends the TOA information to MAC processor **26**A which formats the TOA message and TCP/IP interface **28** sends the message through the wireless network to the master station.

[**0028**] DSP **34** calculates a best-estimate of the TOA for the received signal by performing coherent or non-coherent detection. Coherent detection at the message level is preferred if information about the transmitted message and signal is available such as frequency deviation of the signal and content of the message. In either case, coherent detection is performed at the symbol level by matched filter **32**, providing a high signal to noise ratio (SNR) for the TOA measurement.

[**0029**] The signal/message detection techniques differ in complexity and performance. While coherent detection provides the best theoretical performance, the non-coherent detector represents a simpler implementation with potentially reduced performance. One of the important advantages of the location method described above is its ability to perform well in low signal to noise ratios (SNR). Even if the receiver cannot decode the WLAN message due to noise, the TOA may still be determined with adequate accuracy. Signal energy detection techniques using mean-square estimation as are well known in the art of signal detection may be used to estimate the greatest likelihood arrival time. Other suitable detection algorithms may also be used depending on the type of signals used and the desired complexity of the detection hardware and/or processors.

[**0030**] While the invention has been particularly shown and described with reference to the preferred embodiments thereof, it will be understood by those skilled in the art that the foregoing and other changes in form, and details may be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. A method for determining the location of a wireless device within a wireless local area network (LAN), said method comprising:

receiving a wireless LAN signal from said wireless device at multiple location units;

in response to said receiving, determining multiple times of arrival of said standard wireless LAN signal at each corresponding one of said multiple location units;

sending said times of arrival from each of said corresponding multiple location units to a master unit; and

determining, within said master unit, the location of said wireless device by comparing location information for said multiple location units with said multiple times of arrival to determine said location of said wireless device.

2. The method of claim 1, wherein said master unit is one of said multiple location units, whereby said sending said time of arrival is not performed for said time of arrival determined at said master unit.

3. The method of claim 1, further comprising synchronizing a timer in each of said location units, whereby a precise time relationship between said multiple times of arrival is maintained.

4. The method of claim 1, wherein each of said location units is coupled to said master unit via a wired network, and wherein said sending said times of arrival is performed over said wired network.

5. The method of claim 1, wherein said sending is performed over said wireless network.

6. The method of claim 1, further comprising transmitting a request-to-send signal to said wireless device, and wherein said receiving receives a clear-to-send from said wireless device issued in response to said request-to-send signal.

7. The method of claim 1, wherein said receiving further comprises:

filtering said received signal with a matched filter;

sampling and storing quadrature symbol detection outputs of said matched filter; and

subsequently computing an estimate of said time of arrival of said received signal.

8. The method of claim 7, wherein said computing computes said estimate of said time of arrival in conformity with a maximal mean-square profile of said received signal correlated with a spread-spectrum sequence.

9. The method of claim 6, wherein said computing further computes said estimate of said time of arrival in conformity with a maximal mean-square profile of said received signal convolved with a predetermined message sequence.

10. A wireless local area network (LAN), comprising:

a plurality of location units for receiving a wireless LAN signal transmitted by a wireless device within said wireless LAN and determining a time of arrival for said received signal;

at least one master unit for receiving said time of arrival from each of said location units, whereby said location of said wireless devices is be determined in conformity with said time of arrival.

11. The wireless LAN of claim 10, wherein said master unit is one of said multiple location units.

12. The wireless LAN of claim 10, wherein each of said location units comprises a timebase for maintaining precision in said time of arrival among said location units.

13. The wireless LAN of claim 12, wherein said master unit further synchronizes said timebase in each of said location units by sending a synchronization message to said location units.

14. The wireless LAN of claim 10, wherein each of said location units is coupled to said master unit via a wired network, and wherein said time of arrival is sent from said location units to said master unit over said wired network.

15. The wireless LAN of claim 10, wherein said time of arrival is sent from said location units to said master unit over said wireless network.

16. The wireless LAN of claim 10, further comprising an location measurement initiating unit that transmits a request-to-send signal to said wireless device, and wherein said wireless LAN signal is a clear-to-send message sent from said wireless device in response to said request-to-send signal.

17. The wireless LAN of claim 16, wherein said measurement initiating unit is one of said location units.

18. The wireless LAN of claim 16, wherein said measurement initiating unit is said master unit.

19. The wireless LAN of claim 10, wherein each of said location units comprises a receiver including:

a matched filter for filtering said received signal;

a sampler and memory for sampling and storing quadrature symbol detection outputs of said matched filter; and

a signal processor for computing an estimate of said time of arrival of said received signal from said stored samples.

20. The wireless LAN of claim 19, wherein said signal processor further computes said estimate of said time of arrival in conformity with a maximal mean-square profile of said received signal correlated with a spread-spectrum sequence.

21. The wireless LAN of claim 20, wherein said signal processor further computes said estimate of said time of arrival in conformity with a maximal mean-square profile of said received signal convolved with a predetermined message sequence.

22. A location unit, comprising:

a receiver for receiving wireless local area network (LAN) signals from a wireless device in a wireless network;

a time measurement unit coupled to said receiver for determining the time of arrival of said signals from said wireless device; and

an interface for sending said time of arrival information to a master unit.

23. The location unit of claim 22, wherein said receiver comprises a spread-spectrum receiver and wherein said time measurement unit comprises a processor for determining said time of arrival in conformity with samples stored from an output of said receiver.

24. The location unit of claim 23, wherein said processor computes an estimated time of arrival via mean-square estimation.

25. The location unit of claim 22, wherein said wireless LAN signal is a clear-to-send signal received from said wireless device.

26. A master unit, comprising:

a data interface for receiving from multiple external location units, times of arrival of a standard wireless local area network (LAN) signal received from a wireless device by said multiple external location units;

a database including physical location information of said multiple external location units; and

a computation unit for comparing said times of arrival from said multiple external location units in conformity with location information retrieved from said database to determine a location of wireless devices in a wireless LAN.

27. The master unit of claim 26, wherein said computation unit computes differences between pairs of said time of arrival received from pairs of said location units, projects a hyperbolic curve for each of said differences, said curve having foci at physical locations of said pair of location units associated with a corresponding difference, and determines said location of said wireless device in conformity with an intersection of said hyperbolic curves.

28. The master unit of claim 26, wherein said master unit transmits a command to issue a request-to-send signal to said wireless device over said data interface, and wherein said wireless LAN signal is a clear-to-send signal transmitted by said wireless device in response to said request-to-send signal.

29. The master unit of claim 26, wherein said master unit includes a wireless LAN transmitter, and wherein said master unit transmits a request-to-send signal to said wireless device, and wherein said wireless LAN signal is a clear-to-send signal transmitted by said wireless device in response to said request-to-send signal.

30. The master unit of claim 26, wherein said master unit includes a wireless LAN receiver, and wherein said master unit receives said wireless LAN signal and measures a time of arrival at said master unit of said wireless LAN signal, and wherein said computation unit further compares said time of arrival at said master unit of said wireless LAN signal.

* * * * *