UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SPEIR TECHNOLOGIES LTD., Plaintiff, v. APPLE INC., Defendant.	Case No. 6:22-cv-00077-ADA **JURY TRIAL DEMANDED**

AMENDED COMPLAINT FOR PATENT INFRINGEMENT AGAINST APPLE INC.

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq.*, in which Plaintiff Speir Technologies Limited ("Plaintiff" or "Speir") makes the following allegations against Defendant Apple Inc. ("Defendant" or "Apple"):

INTRODUCTION

1. This amended complaint arises from Apple's unlawful infringement of the following United States patents owned by Plaintiff, which relate to improvements in mobile communications systems: United States Patent Nos. 8,345,780 ("the '780 Patent"), 7,110,779 ("the '779 Patent"), 7,321,777 ("the '777 Patent"), and 7,765,399 ("the '399 Patent") (collectively, the "Asserted Patents").

PARTIES

2. Plaintiff Speir Technologies Limited is a limited liability company organized and existing under the law of Ireland, with its principal place of business at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland. Speir is the sole owner by assignment of all rights,

title, and interest in the Asserted Patents, including the right to recover damages for past, present, and future infringement.

3. On information and belief, Defendant Apple Inc. is a publicly traded corporation organized under the laws of the State of California, with its principal place of business at One Apple Park Way, Cupertino, CA 95014. Apple may be served with process through its registered agent, CT Corporation System, at 818 West Seventh Street, Suite 930, Los Angeles, CA 90017.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Apple in this action because Apple has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Apple would not offend traditional notions of fair play and substantial justice. Apple, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, making, using, importing, offering to sell, and selling products that infringe the Asserted Patents. Apple has not contested personal jurisdiction in this District in prior cases. *See, e.g.*, *Scramoge Tech. Ltd. v. Apple Inc.*, No.6:21-cv-00579-ADA, Dkt. No. 31, ¶ 5 (W.D. Tex. Sept. 14, 2021).

6. Venue is proper in this District under 28 U.S.C. §§ 1391 and 1400(b). Venue is proper in this District under 28 U.S.C. §§ 1391 and 1400(b). Apple is registered to do business in Texas, and upon information and belief, Apple has transacted business in this District and have committed acts of direct and indirect infringement in this District by, among other things, making,

using, offering to sell, selling, and importing products that infringe the Asserted Patents. Apple has regular and established places of business in this District, including at 12545 Riata Vista Cir., Austin, Texas 78727; 12801 Delcour Dr., Austin, Texas 78727; and 3121 Palm Way, Austin, Texas 78758.[1] Apple also has job listings for jobs relating to the accused 5G, Ultra-Wideband ("UWB"), and security technologies in Austin, Texas.[2]

THE ASSERTED PATENTS

7. On January 1, 2013, the United States Patent and Trademark Office issued U.S. Patent No. 8,345,780 ("the '780 Patent"), titled "Wireless communication system compensating for interference and related methods," after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '780 Patent and possesses all rights of recovery under the '780 Patent, including the right to recover damages for past, present, and future infringement. On information and belief, Speir (its predecessors and any licensees) complied with 35 U.S.C. § 287 at all relevant times because Speir (its predecessors and any licensees) do not and did not make, offer for sale, or sell products that practice(d) the '780 Patent. The '780 Patent is valid and enforceable. A true and correct copy of the '780 Patent is attached hereto as Exhibit 1.

---

[1] *See, e.g.*, https://www.apple.com/newsroom/2019/11/apple-expands-in-austin/; https://www.google.com/maps/place/Apple+Inc./@30.4324406,-97.7359733,15z/data=!4m5!3m4!1s0x0:0x5852421ec4ac410c!8m2!3d30.4322558!4d-97.7359386; https://www.apple.com/retail/domainnorthside/.

[2] *See, e.g.*, https://jobs.apple.com/en-us/details/200308092/modem-prototype-system-architect?team=HRDWR; https://jobs.apple.com/en-us/details/200206438/soc-qos-performance-engineer?team=HRDWR; https://jobs.apple.com/en-us/details/200294470/field-design-engineer?team=HRDWR; https://jobs.apple.com/en-us/details/200292503/nfc-uwb-field-design-engineer?team=HRDWR; https://jobs.apple.com/en-us/details/200303024/automation-tools-qa-design-engineer?team=HRDWR; https://jobs.apple.com/en-us/details/200330678/senior-security-engineer?team=SFTWR; https://jobs.apple.com/en-us/details/200344846/security-design-verification-engineer?team=HRDWR.

8. On September 19, 2006, the United States Patent and Trademark Office issued U.S. Patent No. 7,110,779 ("the '779 Patent"), titled "Wireless communication system including a wireless device locator and related methods," after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '779 Patent and possesses all rights of recovery under the '779 Patent, including the right to recover damages for past, present, and future infringement. On information and belief, Speir (its predecessors and any licensees) complied with 35 U.S.C. § 287 at all relevant times because Speir (its predecessors and any licensees) do not and did not make, offer for sale, or sell products that practice(d) the '779 Patent. The '779 Patent is valid and enforceable. A true and correct copy of the '779 Patent is attached hereto as Exhibit 2.

9. On January 22, 2008, the United States Patent and Trademark Office issued U.S. Patent No. 7,321,777 ("the '777 Patent"), titled "Wireless communications system including a wireless device locator and related methods," after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '777 Patent and possesses all rights of recovery under the '777 Patent, including the right to recover damages for past, present, and future infringement. On information and belief, Speir (its predecessors and any licensees) complied with 35 U.S.C. § 287 at all relevant times because Speir (its predecessors and any licensees) do not and did not make, offer for sale, or sell products that practice(d) the '777 Patent. The '777 Patent is valid and enforceable. A true and correct copy of the '777 Patent is attached hereto as Exhibit 3.

10. On July 27, 2010, the United States Patent and Trademark Office issued U.S. Patent No. 7,765,399 ("the '399 Patent"), titled "Computer architecture for a handheld electronic device," after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '399 Patent and possesses all rights of recovery under the '399 Patent, including the right to recover damages for past, present, and future infringement. On information and belief, Speir (its

4

predecessors and any licensees) complied with 35 U.S.C. § 287 at all relevant times because Speir (its predecessors and any licensees) do not and did not make, offer for sale, or sell products that practice(d) the '399 Patent. The '399 Patent is valid and enforceable. A true and correct copy of the '399 Patent is attached hereto as Exhibit 4.

APPLE'S INFRINGEMENT

11. The allegations provided below are exemplary and without prejudice to Plaintiff's infringement contentions provided pursuant to the Court's scheduling order and local rules. Plaintiff's claim construction contentions regarding the meaning and scope of the claim terms will be provided under the Court's scheduling order and local rules. As detailed below, each element of at least one claim of each of the Asserted Patents is literally present in the accused products. To the extent that any element is not literally present, each such element is present under the doctrine of equivalents. Plaintiff's analysis below should not be taken as an admission that the preamble is limiting. While publicly available information is cited below, Plaintiff may rely on other forms of evidence to prove infringement, including evidence that is solely in the possession of Apple and/or third parties.

12. The accused products include at least the following products, as well as products with reasonably similar functionality. Identification of the accused products will be provided in plaintiff's infringement contentions pursuant to the Court's scheduling order and local rules. Apple imports into the United States, uses, makes, offers for sale, and sells in the United States the following products and infringes the asserted claims of the patents-in-suit (the "Accused Products"):

- ’780 Patent Accused Products: iPhone 12, iPhone 12 Mini, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 13, iPhone 13 Mini, iPhone 13 Pro, iPhone 13 Pro Max, iPad Pro, iPad Mini, and any other products with 5G functionality.
- ’779 Patent and ’777 Patent Accused Products: iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone 12, iPhone 12 Mini, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 13, iPhone 13 Mini, iPhone 13 Pro, iPhone 13 Pro Max, AirTags, and any other products with UWB functionality.
- ’399 Patent Accused Products: iPhone 5s and all subsequently released iPhones, iPad Air and all subsequently released models, and MacBook computers with Touch ID.

COUNT I

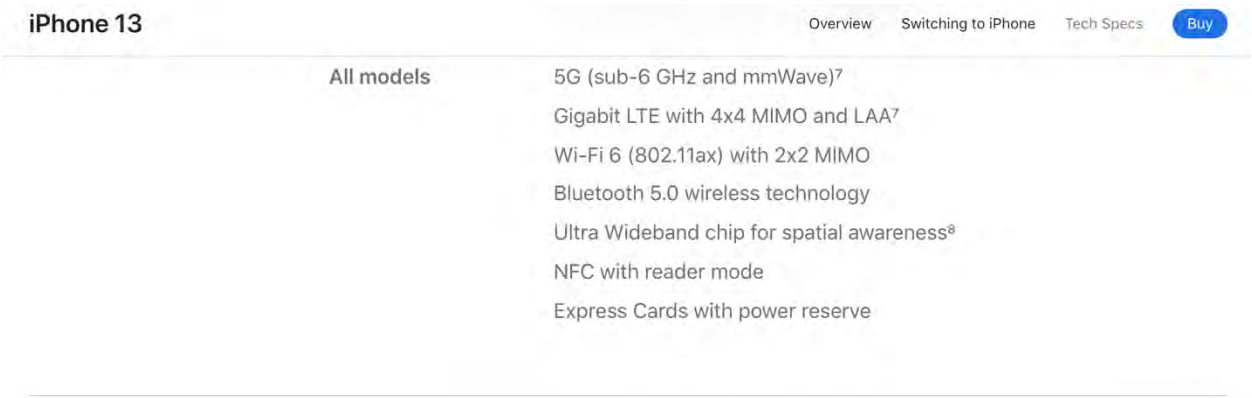
INFRINGEMENT OF U.S. PATENT NO. 8,345,780

13. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

14. Apple has been and is now directly infringing the ’780 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the ’780 Patent, including but not limited to claim 9.

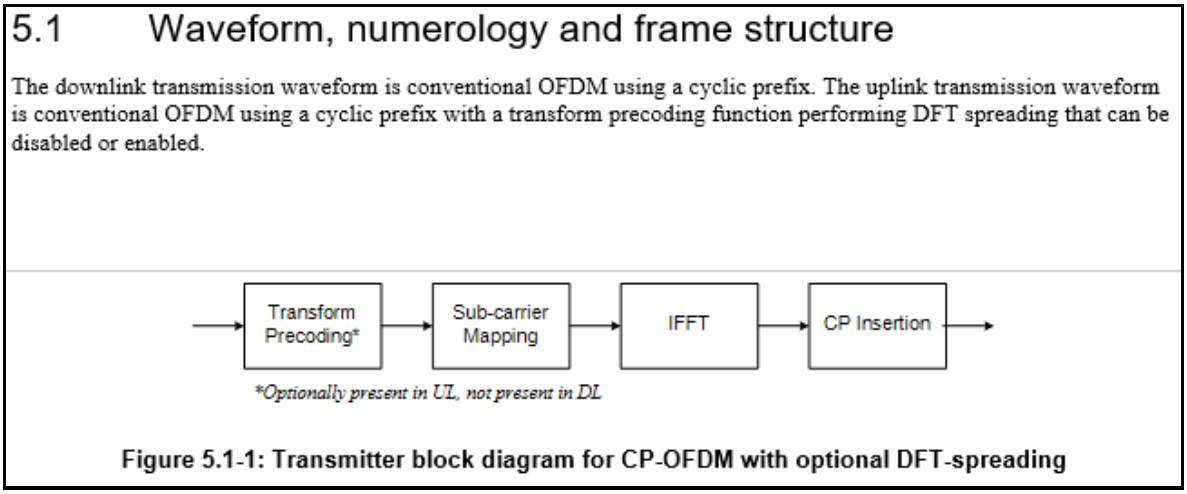
15. Claim 9 of the ’780 Patent recites “[a] wireless communications device operable to communicate with an other wireless communications device via a wireless communications link having at least one settable link characteristic.” To the extent the preamble is limiting, the Accused Products each comprise a wireless communications device operable to communicate with an other wireless communications device via a wireless communications link having at least one settable

link characteristic. For example, the Accused Products are configured to communicate with base stations using 5G cellular technology:



See https://www.apple.com/iphone-13/specs/.

16. Claim 9 of the '780 Patent recites that the "wireless communications device" comprises "an orthogonal frequency-division multiplexing (OFDM) wireless transceiver." The Accused Products each comprise an orthogonal frequency-division multiplexing (OFDM) wireless transceiver. For example, 5G uses OFDM in both the uplink and the downlink:



See 3GPP TS 38.300 V15.13.0.

5.3.1 OFDM baseband signal generation for all channels except PRACH

The time-continuous signal $s_l^{(p,\mu)}(t)$ on antenna port p and subcarrier spacing configuration μ for OFDM symbol $l \in \{0, 1, \ldots, N_{\text{slot}}^{\text{subframe},\mu} N_{\text{symb}}^{\text{slot}} - 1\}$ in a subframe for any physical channel or signal except PRACH is defined by

$$s_l^{(p,\mu)}(t) = \sum_{k=0}^{N_{\text{grid}}^{\text{size},\mu} N_{\text{sc}}^{\text{RB}} - 1} a_{k,l}^{(p,\mu)} \cdot e^{j2\pi\left(k + k_0^{\mu} - N_{\text{grid},x}^{\text{size},\mu} N_{\text{sc}}^{\text{RB}}/2\right)\Delta f\left(t - N_{\text{CP},l}^{\mu} T_c - t_{\text{start},l}^{\mu}\right)}$$

$$k_0^{\mu} = \left(N_{\text{grid},x}^{\text{start},\mu} + N_{\text{grid},x}^{\text{size},\mu}/2\right) N_{\text{sc}}^{\text{RB}} - \left(N_{\text{grid},x}^{\text{start},\mu_0} + N_{\text{grid},x}^{\text{size},\mu_0}/2\right) N_{\text{sc}}^{\text{RB}} 2^{\mu_0 - \mu}$$

where $t_{\text{start},l}^{\mu} \le t < t_{\text{start},l}^{\mu} + \left(N_{\text{u}}^{\mu} + N_{\text{CP},l}^{\mu}\right) T_c$ is the time within the subframe,

$$N_{\text{u}}^{\mu} = 2048\,\kappa \cdot 2^{-\mu}$$

$$N_{\text{CP},l}^{\mu} = \begin{cases} 512\,\kappa \cdot 2^{-\mu} & \text{extended cyclic prefix} \\ 144\,\kappa \cdot 2^{-\mu} + 16\kappa & \text{normal cyclic prefix,} \quad l = 0 \text{ or } l = 7 \cdot 2^{\mu} \\ 144\,\kappa \cdot 2^{-\mu} & \text{normal cyclic prefix,} \quad l \ne 0 \text{ and } l \ne 7 \cdot 2^{\mu} \end{cases}$$

See 3GPP TS 38.211 V15.9.0.

17. Claim 9 of the ’780 Patent recites “a controller coupled to said wireless transceiver and configured to store short term and long term historical characteristics of interference.” The Accused Products each comprise a controller coupled to said wireless transceiver and configured to store short term and long term historical characteristics of interference. For example, the controllers in the Accused Products are configured to store short term and long term historical characteristics of interference:

8

– *CSI-ReportConfig*

The IE *CSI-ReportConfig* is used to configure a periodic or semi-persistent report sent on PUCCH on the cell in which the *CSI-ReportConfig* is included, or to configure a semi-persistent or aperiodic report sent on PUSCH triggered by DCI received on the cell in which the *CSI-ReportConfig* is included (in this case, the cell on which the report is sent is determined by the received DCI). See TS 38.214 [19], clause 5.2.1.

***CSI-ReportConfig* information element**

```
-- ASN1START
-- TAG-CSI-REPORTCONFIG-START

CSI-ReportConfig ::=                SEQUENCE {
    reportConfigId                          CSI-ReportConfigId,
    carrier                                 ServCellIndex                   OPTIONAL,   -- Need S
    resourcesForChannelMeasurement          CSI-ResourceConfigId,
    csi-IM-ResourcesForInterference         CSI-ResourceConfigId            OPTIONAL,   -- Need R
    nzp-CSI-RS-ResourcesForInterference     CSI-ResourceConfigId            OPTIONAL,   -- Need R
    reportConfigType                        CHOICE {
        periodic                                SEQUENCE {
            reportSlotConfig                        CSI-ReportPeriodicityAndOffset,
            pucch-CSI-ResourceList                  SEQUENCE (SIZE (1..maxNrofBWPs)) OF PUCCH-CSI-Resource
        },
        semiPersistentOnPUCCH                   SEQUENCE {
            reportSlotConfig                        CSI-ReportPeriodicityAndOffset,
            pucch-CSI-ResourceList                  SEQUENCE (SIZE (1..maxNrofBWPs)) OF PUCCH-CSI-Resource

        },
        semiPersistentOnPUSCH                   SEQUENCE {
            reportSlotConfig                        ENUMERATED {sl5, sl10, sl20, sl40, sl80, sl160, sl320},
            reportSlotOffsetList                    SEQUENCE (SIZE (1.. maxNrofUL-Allocations)) OF INTEGER(0..32),
            p0alpha                                 P0-PUSCH-AlphaSetId
        },
        aperiodic                               SEQUENCE {
            reportSlotOffsetList                    SEQUENCE (SIZE (1..maxNrofUL-Allocations)) OF INTEGER(0..32)
        }
    },
    reportQuantity                          CHOICE {
        none                                    NULL,
        cri-RI-PMI-CQI                          NULL,
        cri-RI-i1                               NULL,
        cri-RI-i1-CQI                           SEQUENCE {
            pdsch-BundleSizeForCSI                  ENUMERATED {n2, n4}                                     OPTIONAL    -- Need S
        },
        cri-RI-CQI                              NULL,
        cri-RSRP                                NULL,
        ssb-Index-RSRP                          NULL,
        cri-RI-LI-PMI-CQI                       NULL
    },
```

See 3GPP TS 38.331 V15.15.0.

9

***CSI-ReportConfig* field descriptions**
carrier Indicates in which serving cell the *CSI-ResourceConfig* indicated below are to be found. If the field is absent, the resources are on the same serving cell as this report configuration.
codebookConfig Codebook configuration for Type-1 or Type-2 including codebook subset restriction.
cqi-FormatIndicator Indicates whether the UE shall report a single (wideband) or multiple (subband) CQI (see TS 38.214 [19], clause 5.2.1.4).
cqi-Table Which CQI table to use for CQI calculation (see TS 38.214 [19], clause 5.2.2.1).
csi-IM-ResourcesForInterference CSI IM resources for interference measurement. *csi-ResourceConfigId* of a *CSI-ResourceConfig* included in the configuration of the serving cell indicated with the field "carrier" above. The *CSI-ResourceConfig* indicated here contains only CSI-IM resources. The *bwp-Id* in that *CSI-ResourceConfig* is the same value as the *bwp-Id* in the *CSI-ResourceConfig* indicated by *resourcesForChannelMeasurement*.
csi-ReportingBand Indicates a contiguous or non-contiguous subset of subbands in the bandwidth part which CSI shall be reported for. Each bit in the bit-string represents one subband. The right-most bit in the bit string represents the lowest subband in the BWP. The choice determines the number of subbands (subbands3 for 3 subbands, subbands4 for 4 subbands, and so on) (see TS 38.214 [19], clause 5.2.1.4). This field is absent if there are less than 24 PRBs (no sub band) and present otherwise (see TS 38.214 [19], clause 5.2.1.4).
dummy This field is not used in the specification. If received it shall be ignored by the UE.
groupBasedBeamReporting Turning on/off group beam based reporting (see TS 38.214 [19], clause 5.2.1.4).
non-PMI-PortIndication Port indication for RI/CQI calculation. For each CSI-RS resource in the linked ResourceConfig for channel measurement, a port indication for each rank R, indicating which R ports to use. Applicable only for non-PMI feedback (see TS 38.214 [19], clause 5.2.1.4.2). The first entry in *non-PMI-PortIndication* corresponds to the NZP-CSI-RS-Resource indicated by the first entry in *nzp-CSI-RS-Resources* in the *NZP-CSI-RS-ResourceSet* indicated in the first entry of *nzp-CSI-RS-ResourceSetList* of the *CSI-ResourceConfig* whose *CSI-ResourceConfigId* is indicated in a CSI-MeasId together with the above *CSI-ReportConfigId*; the second entry in *non-PMI-PortIndication* corresponds to the NZP-CSI-RS-Resource indicated by the second entry in *nzp-CSI-RS-Resources* in the *NZP-CSI-RS-ResourceSet* indicated in the first entry of *nzp-CSI-RS-ResourceSetList* of the same *CSI-ResourceConfig*, and so on until the NZP-CSI-RS-Resource indicated by the last entry in *nzp-CSI-RS-Resources* in the in the *NZP-CSI-RS-ResourceSet* indicated in the first entry of *nzp-CSI-RS-ResourceSetList* of the same *CSI-ResourceConfig*. Then the next entry corresponds to the NZP-CSI-RS-Resource indicated by the first entry in *nzp-CSI-RS-Resources* in the *NZP-CSI-RS-ResourceSet* indicated in the second entry of *nzp-CSI-RS-ResourceSetList* of the same *CSI-ResourceConfig* and so on.
nrofReportedRS The number (N) of measured RS resources to be reported per report setting in a non-group-based report. N <= N_max, where N_max is either 2 or 4 depending on UE capability. (see TS 38.214 [19], clause 5.2.1.4) When the field is absent the UE applies the value 1.
nzp-CSI-RS-ResourcesForInterference NZP CSI RS resources for interference measurement. *csi-ResourceConfigId* of a *CSI-ResourceConfig* included in the configuration of the serving cell indicated with the field "carrier" above. The *CSI-ResourceConfig* indicated here contains only NZP-CSI-RS resources. The *bwp-Id* in that *CSI-ResourceConfig* is the same value as the *bwp-Id* in the *CSI-ResourceConfig* indicated by *resourcesForChannelMeasurement*.

See 3GPP TS 38.331 V15.15.0.

resourcesForChannelMeasurement Resources for channel measurement. *csi-ResourceConfigId* of a *CSI-ResourceConfig* included in the configuration of the serving cell indicated with the field "carrier" above. The *CSI-ResourceConfig* indicated here contains only NZP-CSI-RS resources and/or SSB resources. This *CSI-ReportConfig* is associated with the DL BWP indicated by *bwp-Id* in that *CSI-ResourceConfig*.
subbandSize Indicates one out of two possible BWP-dependent values for the subband size as indicated in TS 38.214 [19], table 5.2.1.4-2 . If *csi-ReportingBand* is absent, the UE shall ignore this field.
timeRestrictionForChannelMeasurements Time domain measurement restriction for the channel (signal) measurements (see TS 38.214 [19], clause 5.2.1.1).
timeRestrictionForInterferenceMeasurements Time domain measurement restriction for interference measurements (see TS 38.214 [19], clause 5.2.1.1).

See 3GPP TS 38.331 V15.15.0.

Many transmission features in modern radio-access technologies are based on the availability of more or less detailed knowledge about different characteristics of the radio channel over which a signal is to be transmitted. This may range from rough knowledge of the radio-channel path loss for transmit-power adjustment to detailed knowledge about the channel amplitude and phase in the time, frequency, and/or spatial domain. Many transmission features will also benefit from knowledge about the interference level experienced at the receiver side.

Such knowledge about different channel characteristics can be acquired in different ways and by measurements on either the transmitter side or receiver side of a radio link. As an example, knowledge about downlink channel characteristics can be acquired by means of device measurements. The acquired information could then be reported to the network for the setting of different transmission parameters for subsequent downlink transmissions. Alternatively, if it can be assumed that the channel is reciprocal, that is, the channel characteristics of inter-

10

See Erik Dahlman et al., 5G NR: The Next Generation Wireless Access Technology, Ch. 8 Abstract (2d Ed. 2018).

3.7.4 CHANNEL STATE INFORMATION REFERENCE SIGNAL

- The Channel State Information (CSI) Reference Signal is a multi-purpose downlink transmission. The Base Station can configure the UE to use the CSI Reference Signal for one or more of the following:
  - Channel State Information (CSI) Reporting: the UE provides CSI reports to the Base Station based upon measurements from the CSI Reference Signal. For example, the UE derives Channel Quality Indicators (CQI), Rank Indicators (RI) and Precoding Matrix Indicators (PMI) from CSI Reference Signal measurements (Channel State Information is described in section 13.6)

See Chris Johnson, 5G New Radio in Bullets, Section 3.7.4. (2019).

- Figure 186 illustrates an example Multi-User MIMO scenario which involves 3 UE being allocated a common set of Resource Blocks and symbols. Each UE is configured with 2 NZP CSI Reference Signal resources for 'Interference Measurement' and 1 NZP CSI Reference Signal resource for 'Channel Measurement'. The resources are configured such that 2 UE complete interference measurements while the 3rd UE receives its NZP CSI Reference Signal for channel measurement, i.e. 2 UE measure the interference levels generated when transmissions are scheduled towards the 3rd UE. This allows each UE to generate CQI reports which reflect the multi-user MIMO radio conditions

See Chris Johnson, 5G New Radio in Bullets, Section 3.7.4. (2019).

- If a UE is scheduled downlink resources using single user MIMO then interference levels are likely to be dominated by intercell interference (or thermal noise) and so UE measurements should target those sources of interference. 3GPP has specified a third category of CSI Reference Signal resources which can be used for this purpose. These resources are known as **CSI Interference Measurement (IM) Resources**. The Resource Elements configured for this purpose may be used to measure background interference levels, i.e. the serving cell does not transmit anything within these Resource Elements so the UE can measure background interference originating from neighbouring cells

See Chris Johnson, 5G New Radio in Bullets, Section 3.7.4. (2019).

8.1.4: CSI-IM—Resources for Interference Measurements

A configured CSI-RS can be used to derive information about the properties of the channel over which the CSI-RS transmitted. A CSI-RS can also be used to estimate the interference level by subtracting the expected received signal from what is actually received on the CSI-RS resource.

However, the interference level can also be estimated from measurements on so-called *CSI-IM* (Interference Measurement) resources.

See Erik Dahlman et al., 5G NR: The Next Generation Wireless Access Technology, § 8.1.4 (2d Ed. 2018).

11

– *CSI-ReportConfig*

The IE *CSI-ReportConfig* is used to configure a periodic or semi-persistent report sent on PUCCH on the cell in which the *CSI-ReportConfig* is included, or to configure a semi-persistent or aperiodic report sent on PUSCH triggered by DCI received on the cell in which the *CSI-ReportConfig* is included (in this case, the cell on which the report is sent is determined by the received DCI). See TS 38.214 [19], clause 5.2.1.

CSI-ReportConfig information element

```
-- ASN1START
-- TAG-CSI-REPORTCONFIG-START

CSI-ReportConfig ::=                SEQUENCE {
    reportConfigId                          CSI-ReportConfigId,
    carrier                                 ServCellIndex                   OPTIONAL,   -- Need S
    resourcesForChannelMeasurement          CSI-ResourceConfigId,
    csi-IM-ResourcesForInterference         CSI-ResourceConfigId            OPTIONAL,   -- Need R
    nzp-CSI-RS-ResourcesForInterference     CSI-ResourceConfigId            OPTIONAL,   -- Need R
    reportConfigType                        CHOICE {
        periodic                                SEQUENCE {
            reportSlotConfig                        CSI-ReportPeriodicityAndOffset,
            pucch-CSI-ResourceList                  SEQUENCE (SIZE (1..maxNrofBWPs)) OF PUCCH-CSI-Resource
        },
```

See 3GPP TS 38.331 V15.15.0.

18. Claim 9 of the '780 Patent recites that the "controller" is configured to "detect received interference." The Accused Products each comprise a controller configured to detect received interference. For example, the Accused Products are configured to receive the channel state information ("CSI") CSI-ReportConfig parameter structure that informs the user equipment ("UE") of the channel and interference measurements it should make:

- Figure 187 summarises the four categories of CSI Reference Signal resource. These categories are described in greater detail within the following sections. Note that three of the categories are configured within the *CSI-ReportConfig* parameter structure because these categories are associated with UE measurements and reporting. The fourth category is configured within *PDSCH-Config* because this category is used to define Reserved Resources which are not available to the PDSCH

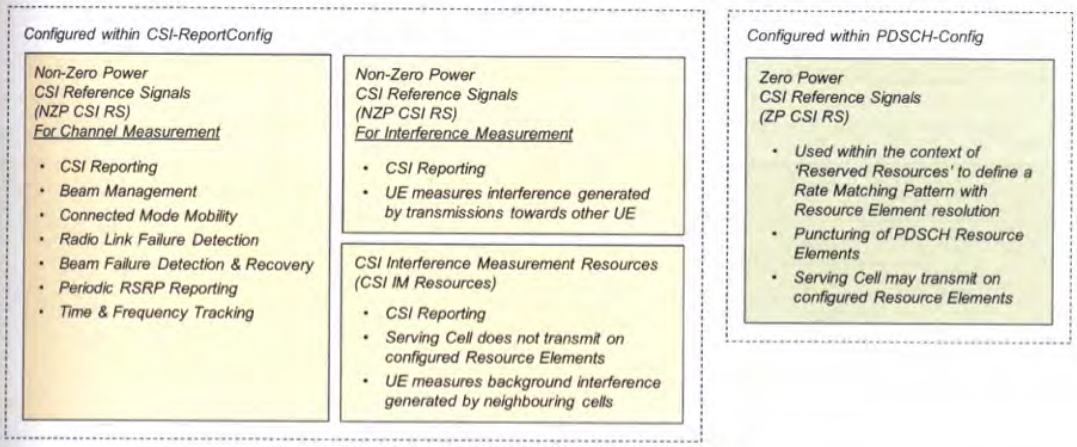


Figure 187 – Categories of CSI Reference Signal

- The *CSI-ReportConfig* parameter structure is used to configure NZP CSI Reference Signal Resources for both Channel Measurement and Interference Measurement. It is also used to configure CSI Interference Measurement (IM) Resources. The hierarchy of parameters associated with the configuration of these resources is illustrated in Figure 188. A set of three information elements corresponding to the three types of resource point towards appropriate instances of *CSI-ResourceConfig*. Instances of *CSI-ResourceConfig* are configured within the *CSI-MeasConfig* parameter structure

See Chris Johnson, 5G New Radio in Bullets, Section 3.7.4. (2019).

12

8.2: Downlink Measurements and Reporting

An NR device can be configured to carry out different measurements, in most cases with corresponding reporting to the network. In general, such a configuration of a measurement and corresponding reporting are done by means of a *report configuration*, in the 3GPP specifications [15] referred to as a *CSI-ReportConfig*.

Each resource configuration describes/indicates:

- The specific quantity or set of quantities to be reported;
- The downlink resource(s) on which measurements should be carried out in order to derive the quantity or quantities to be reported;
- How the actual reporting is to be carried out, for example, when the reporting is to be done and what uplink physical channel to use for the reporting.

See Erik Dahlman et al., 5G NR: The Next Generation Wireless Access Technology, § 8.2 (2d Ed. 2018).

– *CSI-ReportConfig*

The IE *CSI-ReportConfig* is used to configure a periodic or semi-persistent report sent on PUCCH on the cell in which the *CSI-ReportConfig* is included, or to configure a semi-persistent or aperiodic report sent on PUSCH triggered by DCI received on the cell in which the *CSI-ReportConfig* is included (in this case, the cell on which the report is sent is determined by the received DCI). See TS 38.214 [19], clause 5.2.1.

***CSI-ReportConfig* information element**

```
-- ASN1START
-- TAG-CSI-REPORTCONFIG-START

CSI-ReportConfig ::=                SEQUENCE {
    reportConfigId                          CSI-ReportConfigId,
    carrier                                 ServCellIndex                   OPTIONAL,   -- Need S
    resourcesForChannelMeasurement          CSI-ResourceConfigId,
    csi-IM-ResourcesForInterference         CSI-ResourceConfigId            OPTIONAL,   -- Need R
    nzp-CSI-RS-ResourcesForInterference     CSI-ResourceConfigId            OPTIONAL,   -- Need R
    reportConfigType                        CHOICE {
        periodic                                SEQUENCE {
            reportSlotConfig                        CSI-ReportPeriodicityAndOffset,
            pucch-CSI-ResourceList                  SEQUENCE (SIZE (1..maxNrofBWPs)) OF PUCCH-CSI-Resource
        },
        semiPersistentOnPUCCH                   SEQUENCE {
            reportSlotConfig                        CSI-ReportPeriodicityAndOffset,
            pucch-CSI-ResourceList                  SEQUENCE (SIZE (1..maxNrofBWPs)) OF PUCCH-CSI-Resource

        },
        semiPersistentOnPUSCH                   SEQUENCE {
            reportSlotConfig                        ENUMERATED {sl5, sl10, sl20, sl40, sl80, sl160, sl320},
            reportSlotOffsetList                SEQUENCE (SIZE (1.. maxNrofUL-Allocations)) OF INTEGER(0..32),
            p0alpha                                 P0-PUSCH-AlphaSetId
        },
        aperiodic                               SEQUENCE {
            reportSlotOffsetList                SEQUENCE (SIZE (1..maxNrofUL-Allocations)) OF INTEGER(0..32)
        }
    },
```

See 3GPP TS 38.331 V15.15.0.

13

– *CSI-MeasConfig*

The IE *CSI-MeasConfig* is used to configure CSI-RS (reference signals) belonging to the serving cell in which *CSI-MeasConfig* is included, channel state information reports to be transmitted on PUCCH on the serving cell in which *CSI-MeasConfig* is included and channel state information reports on PUSCH triggered by DCI received on the serving cell in which *CSI-MeasConfig* is included. See also TS 38.214 [19], clause 5.2.

CSI-MeasConfig information element

```
-- ASN1START
-- TAG-CSI-MEASCONFIG-START

CSI-MeasConfig ::=                  SEQUENCE {
    nzp-CSI-RS-ResourceToAddModList     SEQUENCE (SIZE (1..maxNrofNZP-CSI-RS-Resources)) OF NZP-CSI-RS-Resource   OPTIONAL, -- Need N
    nzp-CSI-RS-ResourceToReleaseList    SEQUENCE (SIZE (1..maxNrofNZP-CSI-RS-Resources)) OF NZP-CSI-RS-ResourceId OPTIONAL, -- Need N
    nzp-CSI-RS-ResourceSetToAddModList  SEQUENCE (SIZE (1..maxNrofNZP-CSI-RS-ResourceSets)) OF NZP-CSI-RS-ResourceSet
                                                                                                                 OPTIONAL, -- Need N
    nzp-CSI-RS-ResourceSetToReleaseList SEQUENCE (SIZE (1..maxNrofNZP-CSI-RS-ResourceSets)) OF NZP-CSI-RS-ResourceSetId
                                                                                                                 OPTIONAL, -- Need N
    csi-IM-ResourceToAddModList         SEQUENCE (SIZE (1..maxNrofCSI-IM-Resources)) OF CSI-IM-Resource          OPTIONAL, -- Need N
    csi-IM-ResourceToReleaseList        SEQUENCE (SIZE (1..maxNrofCSI-IM-Resources)) OF CSI-IM-ResourceId        OPTIONAL, -- Need N
    csi-IM-ResourceSetToAddModList      SEQUENCE (SIZE (1..maxNrofCSI-IM-ResourceSets)) OF CSI-IM-ResourceSet    OPTIONAL, -- Need N
    csi-IM-ResourceSetToReleaseList     SEQUENCE (SIZE (1..maxNrofCSI-IM-ResourceSets)) OF CSI-IM-ResourceSetId  OPTIONAL, -- Need N
    csi-SSB-ResourceSetToAddModList     SEQUENCE (SIZE (1..maxNrofCSI-SSB-ResourceSets)) OF CSI-SSB-ResourceSet  OPTIONAL, -- Need N
    csi-SSB-ResourceSetToReleaseList    SEQUENCE (SIZE (1..maxNrofCSI-SSB-ResourceSets)) OF CSI-SSB-ResourceSetId OPTIONAL, -- Need N
    csi-ResourceConfigToAddModList      SEQUENCE (SIZE (1..maxNrofCSI-ResourceConfigurations)) OF CSI-ResourceConfig
                                                                                                                 OPTIONAL, -- Need N
    csi-ResourceConfigToReleaseList     SEQUENCE (SIZE (1..maxNrofCSI-ResourceConfigurations)) OF CSI-ResourceConfigId
                                                                                                                 OPTIONAL, -- Need N
    csi-ReportConfigToAddModList        SEQUENCE (SIZE (1..maxNrofCSI-ReportConfigurations)) OF CSI-ReportConfig  OPTIONAL, -- Need N
    csi-ReportConfigToReleaseList       SEQUENCE (SIZE (1..maxNrofCSI-ReportConfigurations)) OF CSI-ReportConfigId
                                                                                                                 OPTIONAL, -- Need N
    reportTriggerSize                   INTEGER (0..6)                                                           OPTIONAL, -- Need M
    aperiodicTriggerStateList           SetupRelease { CSI-AperiodicTriggerStateList }                           OPTIONAL, -- Need M
    semiPersistentOnPUSCH-TriggerStateList    SetupRelease { CSI-SemiPersistentOnPUSCH-TriggerStateList }        OPTIONAL, -- Need M
    ...
}
```

See 3GPP TS 38.331 V15.15.0.

5.2 UE procedure for reporting channel state information (CSI)

5.2.1 Channel state information framework

The time and frequency resources that can be used by the UE to report CSI are controlled by the gNB. CSI may consist of Channel Quality Indicator (CQI), precoding matrix indicator (PMI), CSI-RS resource indicator (CRI), SS/PBCH Block Resource indicator (SSBRI), layer indicator (LI), rank indicator (RI) and/or L1-RSRP.

See 3GPP TS 38.214 V15.14.0.

5.2.1.1 Reporting settings

Each Reporting Setting *CSI-ReportConfig* is associated with a single downlink BWP (indicated by higher layer parameter *BWP-Id*) given in the associated *CSI-ResourceConfig* for channel measurement and contains the parameter(s) for one CSI reporting band:codebook configuration including codebook subset restriction, time-domain behavior, frequency granularity for CQI and PMI, measurement restriction configurations, and the CSI-related quantities to be reported by the UE such as the layer indicator (LI), L1-RSRP, CRI, and SSBRI (SSB Resource Indicator).

The time domain behavior of the *CSI-ReportConfig* is indicated by the higher layer parameter *reportConfigType* and can be set to 'aperiodic', 'semiPersistentOnPUCCH', 'semiPersistentOnPUSCH', or 'periodic'. For periodic and semiPersistentOnPUCCH/semiPersistentOnPUSCH CSI reporting, the configured periodicity and slot offset applies in the numerology of the UL BWP in which the CSI report is configured to be transmitted on. The higher layer parameter *reportQuantity* indicates the CSI-related or L1-RSRP-related quantities to report. The *reportFreqConfiguration* indicates the reporting granularity in the frequency domain, including the CSI reporting band and if PMI/CQI reporting is wideband or sub-band. The *timeRestrictionForChannelMeasurements* parameter in *CSI-ReportConfig* can be configured to enable time domain restriction for channel measurements and *timeRestrictionForInterferenceMeasurements* can be configured to enable time domain restriction for interference measurements. The *CSI-ReportConfig* can also contain *CodebookConfig*, which contains configuration parameters for Type-I or Type II CSI including codebook subset restriction, and configurations of group based reporting.

See 3GPP TS 38.214 V15.14.0.

14

5.2.1.2 Resource settings

Each CSI Resource Setting *CSI-ResourceConfig* contains a configuration of a list of S≥1 CSI Resource Sets (given by higher layer parameter *csi-RS-ResourceSetList*), where the list is comprised of references to either or both of NZP CSI-RS resource set(s) and SS/PBCH block set(s) or the list is comprised of references to CSI-IM resource set(s). Each CSI Resource Setting is located in the DL BWP identified by the higher layer parameter *BWP-id*, and all CSI Resource Settings linked to a CSI Report Setting have the same DL BWP.

The time domain behavior of the CSI-RS resources within a CSI Resource Setting are indicated by the higher layer parameter *resourceType* and can be set to aperiodic, periodic, or semi-persistent. For periodic and semi-persistent CSI Resource Settings, the number of CSI-RS Resource Sets configured is limited to S=1. For periodic and semi-persistent CSI Resource Settings, the configured periodicity and slot offset is given in the numerology of its associated DL BWP, as given by *BWP-id*. When a UE is configured with multiple *CSI-ResourceConfigs* consisting the same NZP CSI-RS resource ID, the same time domain behavior shall be configured for the *CSI-ResourceConfigs*. When a UE is configured with multiple *CSI-ResourceConfigs* consisting the same CSI-IM resource ID, the same time-domain behavior shall be configured for the *CSI-ResourceConfigs*. All CSI Resource Settings linked to a CSI Report Setting shall have the same time domain behavior.

The following are configured via higher layer signaling for one or more CSI Resource Settings for channel and interference measurement:

- CSI-IM resource for interference measurement as described in clause 5.2.2.4.
- NZP CSI-RS resource for interference measurement as described in clause 5.2.2.3.1.
- NZP CSI-RS resource for channel measurement as described in clause 5.2.2.3.1.

See 3GPP TS 38.214 V15.14.0.

7.4.1.5 CSI reference signals

7.4.1.5.1 General

Zero-power (ZP) and non-zero-power (NZP) CSI-RS are defined

- for a non-zero-power CSI-RS configured by the *NZP-CSI-RS-Resource* IE or by the *CSI-RS-Resource-Mobility* field in the *CSI-RS-ResourceConfigMobility* IE, the sequence shall be generated according to clause 7.4.1.5.2 and mapped to resource elements according to clause 7.4.1.5.3
- for a zero-power CSI-RS configured by the *ZP-CSI-RS-Resource* IE, the UE shall assume that the resource elements defined in clause 7.4.1.5.3 are not used for PDSCH transmission subject to clause 5.1.4.2 of [6, TS 38.214]. The UE performs the same measurement/reception on channels/signals except PDSCH regardless of whether they collide with ZP CSI-RS or not.

See 3GPP TS 38.211 V15.9.0.

19. Claim 9 of the '780 Patent recites that the "controller" is configured to "determine a type of the received interference from among a plurality of interference types comprising wideband interference, self interference, and narrowband interference based upon comparing at least one characteristic of a current received signal with the short term and long term historical characteristics of interference." The Accused Products each comprise a controller configured to determine a type of the received interference from among a plurality of interference types comprising wideband interference, self interference, and narrowband interference based upon comparing at least one characteristic of a current received signal with the short term and long term

historical characteristics of interference. For example, the channel state information – reference signal ("CSI-RS") and channel state information – interference measurement ("CSI-IM") resource sets may be specified across the entire bandwidth-part or just a part of the bandwidth that the UE is configured to receive:

> **8.1.2: Frequency-Domain Structure of CSI-RS Configurations**
>
> A CSI-RS is configured for a given downlink bandwidth part and is then assumed to be confined within that bandwidth part and use the numerology of the bandwidth part.
>
> The CSI-RS can be configured to cover the full bandwidth of the bandwidth part or just a fraction of the bandwidth. In the latter case, the CSI-RS bandwidth and frequency-domain starting position are provided as part of the CSI-RS configuration.
>
> Within the configured CSI-RS bandwidth, a CSI-RS may be configured for transmission in every resource block, referred to as *CSI-RS density equal to one*. However, a CSI-RS may also be configured for transmission only in every second resource block, referred to as CSI-RS density equal to 1/2. In the latter case, the CSI-RS configuration includes information about the set of resource blocks (odd resource blocks or even resource blocks) within which the CSI-RS will be transmitted. CSI-RS density equal to 1/2 is not supported for CSI-RS with 4, 8, and 12 antenna ports.

See Erik Dahlman et al., 5G NR: The Next Generation Wireless Access Technology, § 8.1.2 (2d Ed. 2018).

★ The parameter structure used to configure a CSI IM Resource is presented in Table 125. This parameter structure includes a CSI IM Resource identity and a specification of the resources which are allocated to the CSI IM Resource. There is a choice of configuring either pattern 0 or pattern 1:

- Pattern 0 corresponds to a 2×2 grid of Resource Elements. *subcarrierLocation-p0* and *symbolLocation-p0* specify the first subcarrier and first symbol belonging to the 2×2 grid
- Pattern 1 corresponds to a 4×1 grid of Resource Elements (4 subcarriers × 1 symbol). *subcarrierLocation-p1* and *symbolLocation-p1* specify the first subcarrier and the only symbol belonging to the 4×1 grid

Examples of patterns 0 and 1 are illustrated in Figure 199

CSI-IM-Resource						
csi-IM-ResourceId	0 to 31					
csi-IM-ResourceElementPattern	CHOICE					
	pattern0			pattern1		
	subcarrierLocation-p0	0, 2, 4, 6, 8 10		subcarrierLocation-p1	0, 4, 8	
	symbolLocation-p0	0 to 12		symbolLocation-p1	0 to 13	
freqBand	startingRB	0 to 274, step 4				
	nrofRBs	24 to 276, step 4				
periodicityAndOffset	CHOICE					
	4 slots	0 to 3	20 slots	0 to 19	160 slots	0 to 159
	5 slots	0 to 4	32 slots	0 to 31	320 slots	0 to 319
	8 slots	0 to 7	40 slots	0 to 39	640 slots	0 to 639
	10 slots	0 to 9	64 slots	0 to 63		
	16 slots	0 to 15	80 slots	0 to 79		

Table 125 – Parameter structure used to configure a CSI IM Resource

★ The *freqBand* section of the parameter structure specifies the set of contiguous Resource Blocks across which the CSI IM Resource is configured. The *startingRB* is relative to Common Resource Block 0, i.e. the lower edge of the channel bandwidth, rather than the lower edge of the Bandwidth Part. The *nrofRBs* information element has a minimum value of 24 but if the Bandwidth Part occupies less than 24 Resource Blocks then the CSI IM Resource occupies only the Resource Blocks within the Bandwidth Part

See Chris Johnson, 5G New Radio in Bullets, Section 3.7.4. (2019).

– *NZP-CSI-RS-Resource*

The IE *NZP-CSI-RS-Resource* is used to configure Non-Zero-Power (NZP) CSI-RS transmitted in the cell where the IE is included, which the UE may be configured to measure on (see TS 38.214 [19], clause 5.2.2.3.1). A change of configuration between periodic, semi-persistent or aperiodic for an *NZP-CSI-RS-Resource* is not supported without a release and add.

***NZP-CSI-RS-Resource* information element**

```
-- ASN1START
-- TAG-NZP-CSI-RS-RESOURCE-START

NZP-CSI-RS-Resource ::=             SEQUENCE {
    nzp-CSI-RS-ResourceId               NZP-CSI-RS-ResourceId,
    resourceMapping                     CSI-RS-ResourceMapping,
    powerControlOffset                  INTEGER (-8..15),
    powerControlOffsetSS                ENUMERATED{db-3, db0, db3, db6}                 OPTIONAL,   -- Need R
    scramblingID                        ScramblingId,
    periodicityAndOffset                CSI-ResourcePeriodicityAndOffset                OPTIONAL,   -- Cond PeriodicOrSemiPersistent
    qcl-InfoPeriodicCSI-RS              TCI-StateId                                     OPTIONAL,   -- Cond Periodic
    ...
}
```

See 3GPP TS 38.331 V 15.15.0.

– *CSI-IM-Resource*

The IE *CSI-IM-Resource* is used to configure one CSI Interference Management (IM) resource.

***CSI-IM-Resource* information element**

```
-- ASN1START
-- TAG-CSI-IM-RESOURCE-START

CSI-IM-Resource ::=                 SEQUENCE {
    csi-IM-ResourceId                   CSI-IM-ResourceId,
    csi-IM-ResourceElementPattern           CHOICE {
        pattern0                                SEQUENCE {
            subcarrierLocation-p0                   ENUMERATED { s0, s2, s4, s6, s8, s10 },
            symbolLocation-p0                       INTEGER (0..12)
        },
        pattern1                                SEQUENCE {
            subcarrierLocation-p1                   ENUMERATED { s0, s4, s8 },
            symbolLocation-p1                       INTEGER (0..13)
        }
    }                                                                       OPTIONAL,   -- Need M
    freqBand                            CSI-FrequencyOccupation             OPTIONAL,   -- Need M
    periodicityAndOffset                CSI-ResourcePeriodicityAndOffset    OPTIONAL,   -- Cond PeriodicOrSemiPersistent
    ...
}
```

See 3GPP TS 38.331 V 15.15.0.

18

5.2.2.3.1 NZP CSI-RS

The UE can be configured with one or more NZP CSI-RS resource set configuration(s) as indicated by the higher layer parameters *CSI-ResourceConfig,* and *NZP-CSI-RS-ResourceSet.* Each NZP CSI-RS resource set consists of $K \geq 1$ NZP CSI-RS resource(s).

The following parameters for which the UE shall assume non-zero transmission power for CSI-RS resource are configured via the higher layer parameter *NZP-CSI-RS-Resource, CSI-ResourceConfig* and *NZP-CSI-RS-ResourceSet* for each CSI-RS resource configuration:

- *nzp-CSI-RS-ResourceId* determines CSI-RS resource configuration identity.
- *periodicityAndOffset* defines the CSI-RS periodicity and slot offset for periodic/semi-persistent CSI-RS. All the CSI-RS resources within one set are configured with the same periodicity, while the slot offset can be same or different for different CSI-RS resources.
- *resourceMapping* defines the number of ports, CDM-type, and OFDM symbol and subcarrier occupancy of the CSI-RS resource within a slot that are given in clause 7.4.1.5 of [4, TS 38.211].
- *nrofPorts* in *resourceMapping* defines the number of CSI-RS ports, where the allowable values are given in clause 7.4.1.5 of [4, TS 38.211].
- *density* in *resourceMapping* defines CSI-RS frequency density of each CSI-RS port per PRB, and CSI-RS PRB offset in case of the density value of 1/2, where the allowable values are given in clause 7.4.1.5 of [4, TS 38.211]. For density 1/2, the odd/even PRB allocation indicated in *density* is with respect to the common resource block grid.
- *cdm-Type* in *resourceMapping* defines CDM values and pattern, where the allowable values are given in clause 7.4.1.5 of [4, TS 38.211].
- *powerControlOffset*: which is the assumed ratio of PDSCH EPRE to NZP CSI-RS EPRE when UE derives CSI feedback and takes values in the range of [-8, 15] dB with 1 dB step size.
- *powerControlOffsetSS*: which is the assumed ratio of NZP CSI-RS EPRE to SS/PBCH block EPRE.
- *scramblingID* defines scrambling ID of CSI-RS with length of 10 bits.
- *BWP-Id* in *CSI-ResourceConfig* defines which bandwidth part the configured CSI-RS is located in.
- *repetition* in *NZP-CSI-RS-ResourceSet* is associated with a CSI-RS resource set and defines whether UE can assume the CSI-RS resources within the NZP CSI-RS Resource Set are transmitted with the same downlink spatial domain transmission filter or not as described in clause 5.1.6.1.2. and can be configured only when the higher layer parameter *reportQuantity* associated with all the reporting settings linked with the CSI-RS resource set is set to 'cri-RSRP' or 'none'.
- *qcl-InfoPeriodicCSI-RS* contains a reference to a *TCI-State* indicating QCL source RS(s) and QCL type(s). If the *TCI-State* is configured with a reference to an RS with 'QCL-TypeD' association, that RS may be an SS/PBCH block located in the same or different CC/DL BWP or a CSI-RS resource configured as periodic located in the same or different CC/DL BWP.
- *trs-Info* in *NZP-CSI-RS-ResourceSet* is associated with a CSI-RS resource set and for which the UE can assume that the antenna port with the same port index of the configured NZP CSI-RS resources in the *NZP-CSI-RS-ResourceSet* is the same as described in clause 5.1.6.1.1 and can be configured when reporting setting is not configured or when the higher layer parameter *reportQuantity* associated with all the reporting settings linked with the CSI-RS resource set is set to 'none'.

See 3GPP TS 38.214 V15.14.0.

19

All CSI-RS resources within one set are configured with same *density* and same *nrofPorts*, except for the NZP CSI-RS resources used for interference measurement.

The UE expects that all the CSI-RS resources of a resource set are configured with the same starting RB and number of RBs and the same *cdm-type*.

The bandwidth and initial common resource block (CRB) index of a CSI-RS resource within a BWP, as defined in clause 7.4.1.5 of [4, TS 38.211], are determined based on the higher layer parameters *nrofRBs* and *startingRB*, respectively, within the CSI-FrequencyOccupation IE configured by the higher layer parameter *freqBand* within the *CSI-RS-ResourceMapping* IE. Both *nrofRBs* and *startingRB* are configured as integer multiples of 4 RBs, and the reference point for *startingRB* is CRB 0 on the common resource block grid. If $startingRB < N_{BWP}^{start}$, the UE shall assume that the initial CRB index of the CSI-RS resource is $N_{initial\ RB} = N_{BWP}^{start}$, otherwise $N_{initial\ RB} = startingRB$. If $nrofRBs > N_{BWP}^{size} + N_{BWP}^{start} - N_{initial\ RB}$, the UE shall assume that the bandwidth of the CSI-RS resource is $N_{CSI-RS}^{BW} = N_{BWP}^{size} + N_{BWP}^{start} - N_{initial\ RB}$, otherwise $N_{CSI-RS}^{BW} = nrofRBs$. In all cases, the UE shall expect that $N_{CSI-RS}^{BW} \geq \min(24, N_{BWP}^{size})$.

See 3GPP TS 38.214 V15.14.0.

5.2.2.4 Channel State Information – Interference Measurement (CSI-IM)

The UE can be configured with one or more CSI-IM resource set configuration(s) as indicated by the higher layer parameter *CSI-IM-ResourceSet*. Each CSI-IM resource set consists of $K \geq 1$ CSI-IM resource(s).

The following parameters are configured via higher layer parameter *CSI-IM-Resource* for each CSI-IM resource configuration:

- *csi-IM-ResourceId* determines CSI-IM resource configuration identity
- *subcarrierLocation-p0* or *subcarrierLocation-p1* defines subcarrier occupancy of the CSI-IM resource within a slot for *csi-IM-ResourceElementPattern* set to 'pattern0' or 'pattern1', respectively.
- *symbolLocation-p0* or *symbolLocation-p1* defines OFDM symbol location of the CSI-IM resource within a slot for *csi-IM-ResourceElementPattern* set to 'pattern0' or 'pattern1', respectively.
- *periodicityAndOffset* defines the CSI-IM periodicity and slot offset for periodic/semi-persistent CSI-IM.
- *freqBand* includes parameters to enable configuration of frequency-occupancy of CSI-IM

In each of the PRBs configured by *freqBand*, the UE shall assume each CSI-IM resource is located in,

- resource elements (k_{CSI-IM}, l_{CSI-IM}), $(k_{CSI-IM}, l_{CSI-IM}+1)$, $(k_{CSI-IM}+1, l_{CSI-IM})$ and $(k_{CSI-IM}+1, l_{CSI-IM}+1)$, if *csi-IM-ResourceElementPattern* is set to 'pattern0',
- resource elements (k_{CSI-IM}, l_{CSI-IM}), $(k_{CSI-IM}+1, l_{CSI-IM})$, $(k_{CSI-IM}+2, l_{CSI-IM})$ and $(k_{CSI-IM}+3, l_{CSI-IM})$ if *csi-IM-ResourceElementPattern* is set to 'pattern1',

where k_{CSI-IM} and l_{CSI-IM} are the configured frequency-domain location and time-domain location, respectively, given by the higher layer parameters in the above list.

See 3GPP TS 38.214 V15.14.0.

For example, channel measurements such as CQI are based upon either multiple in time or single time readings.

20

5.2.2 Channel state information

5.2.2.1 Channel quality indicator (CQI)

The CQI indices and their interpretations are given in Table 5.2.2.1-2 or Table 5.2.2.1-4 for reporting CQI based on QPSK, 16QAM and 64QAM. The CQI indices and their interpretations are given in Table 5.2.2.1-3 for reporting CQI based on QPSK, 16QAM, 64QAM and 256QAM.

Based on an unrestricted observation interval in time unless specified otherwise in this clause, and an unrestricted observation interval in frequency, the UE shall derive for each CQI value reported in uplink slot *n* the highest CQI index which satisfies the following condition:

- A single PDSCH transport block with a combination of modulation scheme, target code rate and transport block size corresponding to the CQI index, and occupying a group of downlink physical resource blocks termed the CSI reference resource, could be received with a transport block error probability not exceeding:
  - 0.1, if the higher layer parameter *cqi-Table* in *CSI-ReportConfig* configures 'table1' (corresponding to Table 5.2.2.1-2), or 'table2' (corresponding to Table 5.2.2.1-3), or
  - 0.00001, if the higher layer parameter *cqi-Table* in *CSI-ReportConfig* configures 'table3' (corresponding to Table 5.2.2.1-4).

If higher layer parameter *timeRestrictionForChannelMeasurements* is set to "*notConfigured*", the UE shall derive the channel measurements for computing CSI value reported in uplink slot n based on only the NZP CSI-RS, no later than the CSI reference resource, (defined in TS 38.211[4]) associated with the CSI resource setting.

If higher layer parameter *timeRestrictionForChannelMeasurements* in *CSI-ReportConfig* is set to "*Configured*", the UE shall derive the channel measurements for computing CSI reported in uplink slot n based on only the most recent, no later than the CSI reference resource, occasion of NZP CSI-RS (defined in [4, TS 38.211]) associated with the CSI resource setting.

If higher layer parameter *timeRestrictionForInterferenceMeasurements* is set to "*notConfigured*", the UE shall derive the interference measurements for computing CSI value reported in uplink slot n based on only the CSI-IM and/or NZP CSI-RS for interference measurement no later than the CSI reference resource associated with the CSI resource setting.

If higher layer parameter *timeRestrictionForInterferenceMeasurements* in *CSI-ReportConfig* is set to "*Configured*", the UE shall derive the interference measurements for computing the CSI value reported in uplink slot n based on the most recent, no later than the CSI reference resource, occasion of CSI-IM and/or NZP CSI-RS for interference measurement (defined in [4, TS 38.211]) associated with the CSI resource setting.

See 3GPP TS 38.214 §5.2.2.1.

For example, rank indicator ("RI") and pre-coding matrix indicator ("PMI") are also computed based on SRS measurements.

> To select a suitable rank and a corresponding precoder matrix, the network needs estimates of the channels between the device antenna ports and the corresponding network receive antennas. To enable this, a device configured for codebook-based PUSCH would typically be configured for transmission of at least one multi-port SRS. Based on measurements on the configured SRS, the network can sound the channel and determine a suitable rank and precoder matrix.

21

See Erik Dahlman et al., 5G NR: The Next Generation Wireless Access Technology, § 11.3.1 (2d Ed. 2018).

20. Claim 9 of the '780 Patent recites that the "controller" is configured to "set the at least one settable link characteristic to compensate for the received interference based upon the interference type." The Accused Products each comprise a controller configured to set the at least one settable link characteristic to compensate for the received interference based upon the interference type. For example, the Accused Products report at least wideband and subband CQI, wideband and subband PMI, and also RI:

> - wideband CQI or subband CQI reporting, as configured by the higher layer parameter *cqi-FormatIndicator*. When wideband CQI reporting is configured, a wideband CQI is reported for each codeword for the entire CSI reporting band. When subband CQI reporting is configured, one CQI for each codeword is reported for each subband in the CSI reporting band.

See 3GPP TS 38.214 V.15.14.0 §5.2.1.4.

> wideband PMI or subband PMI reporting as configured by the higher layer parameter *pmi-FormatIndicator*. When wideband PMI reporting is configured, a wideband PMI is reported for the entire CSI reporting band. When subband PMI reporting is configured, except with 2 antenna ports, a single wideband indication (i_1 in clause 5.2.2.2) is reported for the entire CSI reporting band and one subband indication (i_2 in clause 5.2.2.2) is reported for each subband in the CSI reporting band. When subband PMIs are configured with 2 antenna ports, a PMI is reported for each subband in the CSI reporting band.

See 3GPP TS 38.214 V.15.14.0 §5.2.1.4.

22

5.2.2.1 Channel quality indicator (CQI)

The CQI indices and their interpretations are given in Table 5.2.2.1-2 or Table 5.2.2.1-4 for reporting CQI based on QPSK, 16QAM and 64QAM. The CQI indices and their interpretations are given in Table 5.2.2.1-3 for reporting CQI based on QPSK, 16QAM, 64QAM and 256QAM.

Based on an unrestricted observation interval in time unless specified otherwise in this clause, and an unrestricted observation interval in frequency, the UE shall derive for each CQI value reported in uplink slot *n* the highest CQI index which satisfies the following condition:

- A single PDSCH transport block with a combination of modulation scheme, target code rate and transport block size corresponding to the CQI index, and occupying a group of downlink physical resource blocks termed the CSI reference resource, could be received with a transport block error probability not exceeding:
  - 0.1, if the higher layer parameter *cqi-Table* in *CSI-ReportConfig* configures 'table1' (corresponding to Table 5.2.2.1-2), or 'table2' (corresponding to Table 5.2.2.1-3), or
  - 0.00001, if the higher layer parameter *cqi-Table* in *CSI-ReportConfig* configures 'table3' (corresponding to Table 5.2.2.1-4).

If higher layer parameter *timeRestrictionForChannelMeasurements* is set to "*notConfigured*", the UE shall derive the channel measurements for computing CSI value reported in uplink slot n based on only the NZP CSI-RS, no later than the CSI reference resource, (defined in TS 38.211[4]) associated with the CSI resource setting.

If higher layer parameter *timeRestrictionForChannelMeasurements* in *CSI-ReportConfig* is set to "*Configured*", the UE shall derive the channel measurements for computing CSI reported in uplink slot n based on only the most recent, no later than the CSI reference resource, occasion of NZP CSI-RS (defined in [4, TS 38.211]) associated with the CSI resource setting.

If higher layer parameter *timeRestrictionForInterferenceMeasurements* is set to "*notConfigured*", the UE shall derive the interference measurements for computing CSI value reported in uplink slot n based on only the CSI-IM and/or NZP CSI-RS for interference measurement no later than the CSI reference resource associated with the CSI resource setting.

See 3GPP TS 38.214 V.15.14.0.

The bitwidth for RI/LI/CQI/CRI of *codebookType=typeI-SinglePanel* is provided in Tables 6.3.1.1.2-3.

Table 6.3.1.1.2-3: RI, LI, CQI, and CRI of *codebookType=typeI-SinglePanel*

Field	Bitwidth				
	1 antenna port	2 antenna ports	4 antenna ports	>4 antenna ports	
				Rank1~4	Rank5~8
Rank Indicator	0	$\min(1,\lceil \log_2 n_{RI} \rceil)$	$\min(2,\lceil \log_2 n_{RI} \rceil)$	$\lceil \log_2 n_{RI} \rceil$	$\lceil \log_2 n_{RI} \rceil$
Layer Indicator	0	$\lceil \log_2 \upsilon \rceil$	$\min(2,\lceil \log_2 \upsilon \rceil)$	$\min(2,\lceil \log_2 \upsilon \rceil)$	$\min(2,\lceil \log_2 \upsilon \rceil)$
Wide-band CQI for the first TB	4	4	4	4	4
Wideband CQI for the second TB	0	0	0	0	4
Subband differential CQI for the first TB	2	2	2	2	2
Subband differential CQI for the second TB	0	0	0	0	2
CRI	$\lceil \log_2(K_s^{CSI-RS}) \rceil$	$\lceil \log_2(K_s^{CSI-RS}) \rceil$	$\lceil \log_2(K_s^{CSI-RS}) \rceil$	$\lceil \log_2(K_s^{CSI-RS}) \rceil$	$\lceil \log_2(K_s^{CSI-RS}) \rceil$

n_{RI} in Table 6.3.1.1.2-3 is the number of allowed rank indicator values according to Clause 5.2.2.2.1 [6, TS 38.214].

υ is the value of the rank. The value of K_s^{CSI-RS} is the number of CSI-RS resources in the corresponding resource set.

The values of the rank indicator field are mapped to allowed rank indicator values with increasing order, where '0' is mapped to the smallest allowed rank indicator value.

23

See 3GPP TS 38.212 V15.12.0 §6.3.1.1.2.

21. Apple also knowingly and intentionally induces infringement of one or more claims of the '780 Patent in violation of 35 U.S.C. § 271(b). At least as of the filing and service of this amended complaint, Apple has knowledge of the '780 Patent and the infringing nature of the Accused Products. For example, Apple obtained knowledge of the '780 Patent at least as of January 21, 2022 when it was served with the initial complaint. Dkt. No. 6. Despite this knowledge of the '780 Patent, Apple continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '780 Patent, for example by utilizing the accused 5G functionality on the Accused Products in an infringing manner. *See, e.g.*, https://support.apple.com/en-gb/guide/iphone/iph3dd5f213/15.0/ios/15.0 (Apple iPhone 13 User Manual – "View or change cellular data settings on iPhone"). Further, Apple advertises to customers that "[n]o one does 5G like iPhone." https://www.apple.com/iphone-13/. Apple provides these instructions and online materials to customers and end users knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Apple also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '780 Patent, thereby specifically intending for and inducing its customers to infringe the '780 Patent through the customers' normal and customary use of the Accused Products.

22. Apple has also infringed, and continues to infringe, one or more claims of the '780 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '780 Patent, are especially made or adapted to infringe the '780 Patent, and are not staple articles or

commodities of commerce suitable for non-infringing use (as exemplified by the materials cited above). At least as of the filing and service of this amended complaint, Apple has knowledge of the '780 Patent and the infringing nature of the Accused Products. Apple has been, and currently is, contributorily infringing the '780 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

23. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Apple has injured Plaintiff and is liable for infringement of the '780 Patent pursuant to 35 U.S.C. § 271.

24. As a result of Apple's direct infringement of the '780 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

25. As a result of Apple's indirect infringement of the '780 Patent (induced and contributory), Plaintiff is entitled to monetary damages (present and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

COUNT II

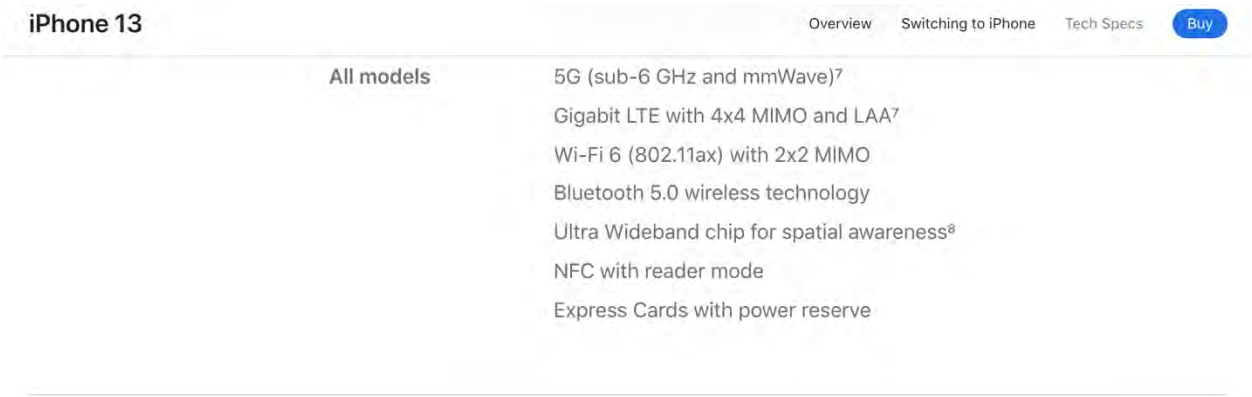
INFRINGEMENT OF U.S. PATENT NO. 7,110,779

26. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

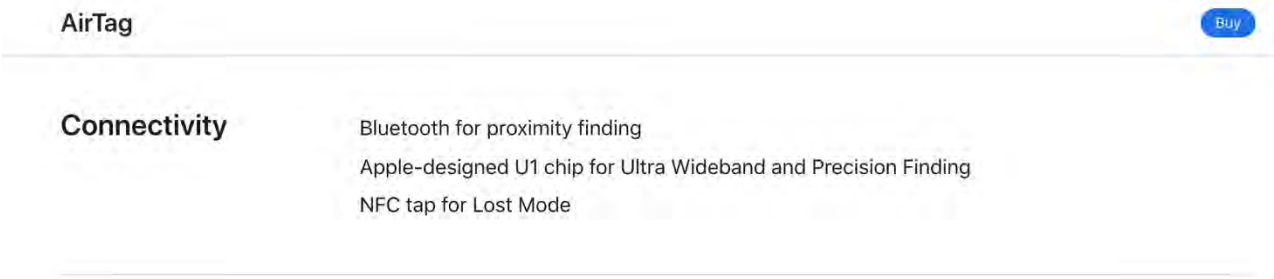
27. Apple has been and is now directly infringing the '779 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products and systems, including at least the Accused Products identified above. The Accused Products

satisfy all of the claim limitations of one or more claims of the '779 Patent, including but not limited to claim 18.

28. Claim 18 of the '779 Patent recites "[a] wireless device locator for locating a target wireless communications device having a unique identifier (UID) associated therewith." To the extent the preamble is limiting, the Accused Products each comprise a wireless device locator for locating a target wireless communications device having a unique identifier (UID) associated therewith. For example, the accused Apple iPhone 13 supports ultra-wideband functionality for locating a target wireless communications device, such as the Apple AirTag:

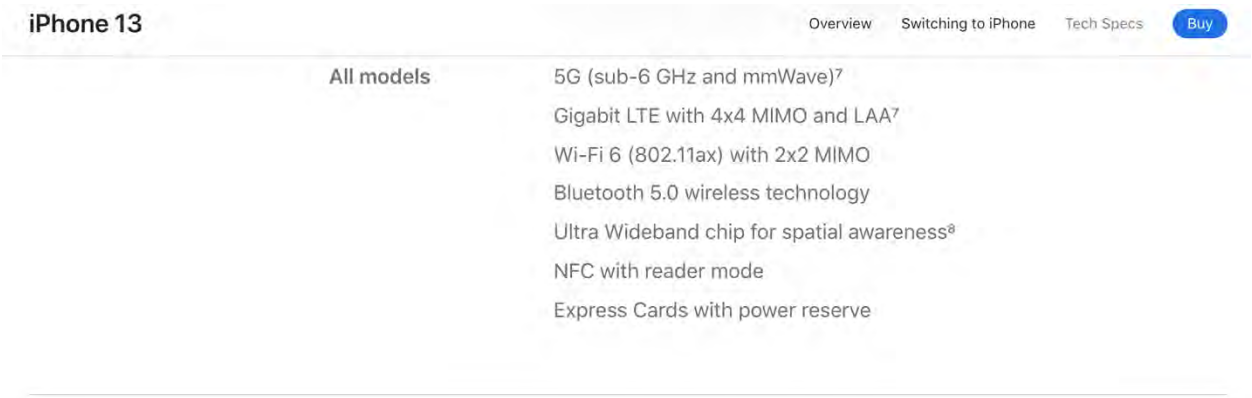


See https://www.apple.com/iphone-13/specs/.



See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

29. Claim 18 of the '779 Patent recites "at least one antenna and a transceiver connected thereto." The Accused Products comprise at least one antenna and a transceiver connected thereto. For example, the iPhone 13 comprises at least one antenna and a transceiver:



See https://www.apple.com/iphone-13/specs/.

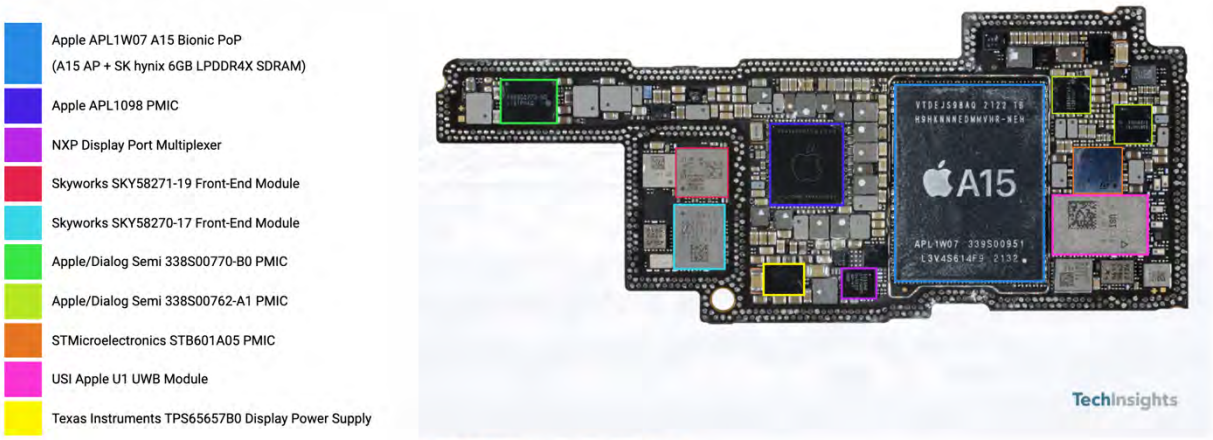
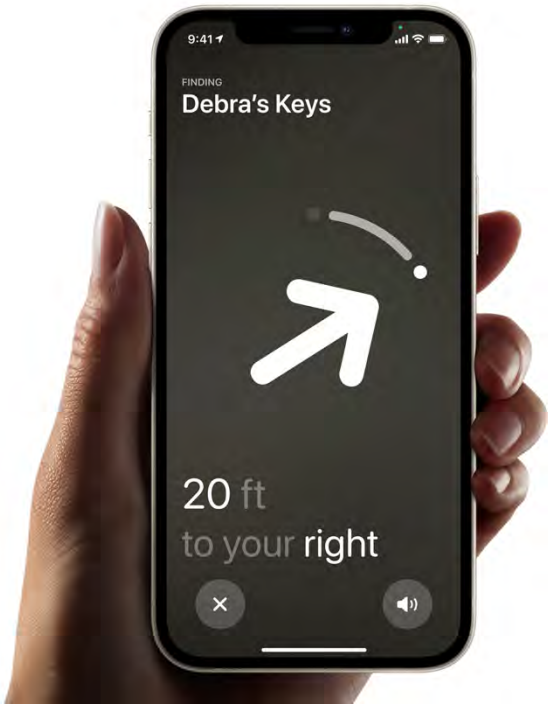


Figure 1. Apple iPhone Pro Board Shot

See https://www.techinsights.com/blog/teardown/apple-iphone-13-pro-teardown.

30. Claim 18 of the '779 Patent recites "a controller for" "cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device, inserting the UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of said location finding signals generated by the target wireless communications device based upon the UID in the

location finding signals." The Accused Products comprise a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device, inserting the UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of said location finding signals generated by the target wireless communications device based upon the UID in the location finding signals. For example, on information and belief, the iPhone 13 comprises a controller that cooperates with a transceiver and includes a UID for the target wireless communications device (such as an Apple AirTag) in location finding signals:



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

7.2 General MAC frame format

7.2.1 General

The general MAC frame for Frame Type values other than fragment and extended, as defined in Table 7-1, shall be formatted as illustrated in Figure 7-1.

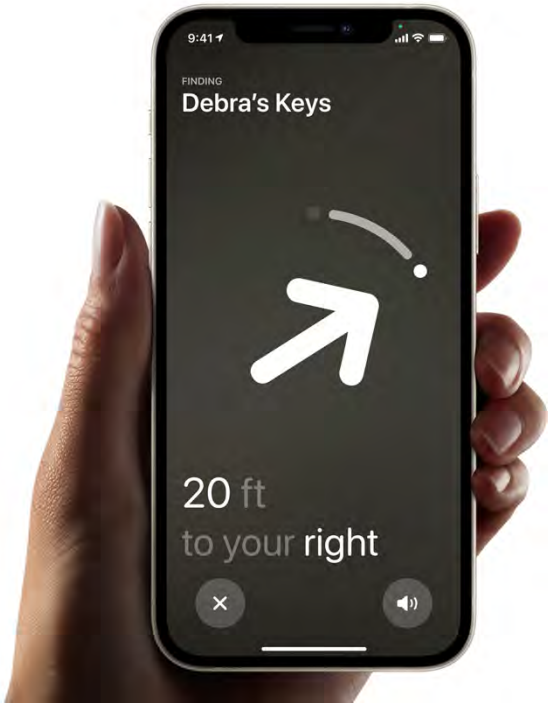
Octets: 1/2	0/1	0/2	0/2/8	0/2	0/2/8	variable	variable		variable	2/4
Frame Control	Sequence Number	Destination PAN ID	Destination Address	Source PAN ID	Source Address	Auxiliary Security Header	IE		Frame Payload	FCS
		Addressing fields					Header IEs	Payload IEs		
MHR								MAC Payload		MFR

Figure 7-1—General MAC frame format

29

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Section 7.2.1.

31. Claim 18 of the '779 Patent recites a "controller for" "determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device." The Accused Products comprise a controller for determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device. For example, the Apple iPhone 13 comprises a controller for determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device (such as an Apple AirTag):



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

31

6.9.1.2.2 Single-sided two-way ranging (SS-TWR)

SS-TWR involves a measurement of the round-trip delay of a single message from one device to another and a response sent back to the original device. The operation of SS-TWR is as shown in Figure 6-47a, where device A initiates the exchange and device B responds to complete the exchange and T_{prop} is the propagation time of the RMARKER between the devices.

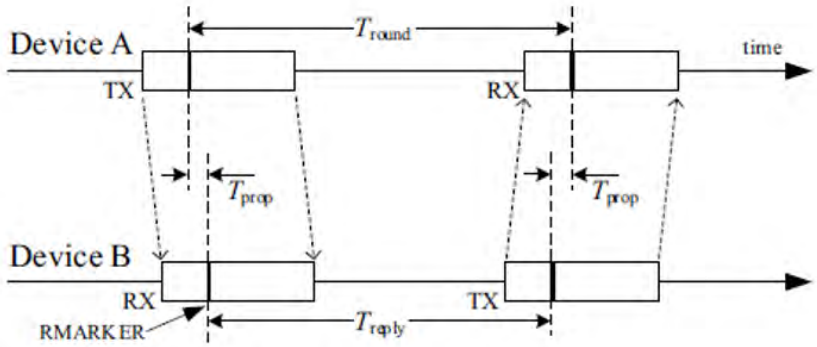


Figure 6-47a—SS-TWR

Each device precisely measures the transmission and reception times of the message frames, and so can calculate times T_{round} and T_{reply} by simple subtraction. Hence, the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

$$\hat{T}_{prop} = \frac{1}{2}(T_{round} - T_{reply})$$

* * *

When employing SS-TWR, for the TOF to be calculated at device A, device A needs the reply time T_{reply} employed by device B. When T_{reply} is determined by device B after its transmission, an additional message is necessary to bring this value to device A, as shown in Figure 6-48a and described in 6.9.6.3. When T_{reply} can be accurately predicted by device B before its transmission, the value can be embedded in the reply message itself, as shown in Figure 6-48b and described in 6.9.6.4. Alternatively, if device B has the ability to always reply with sufficiently accurate constant or pre-known reply time, it obviates the need for any transfer of T_{reply} as part of the ranging exchange, as described in 6.9.6.5.

* * *

32

6.9.1.2.3 Double-sided two-way ranging (DS-TWR)

DS-TWR is an extension of SS-TWR in which two round-trip time measurements are used and combined to give the TOF result with a reduced error in the presence of uncorrected clock frequency offset even for quite long response delays. The operation of DS-TWR is shown in Figure 6-47b, where device A initiates the first round-trip time measurement to which device B responds, after which device B initiates the second round-trip time measurement to which device A responds completing the full DS-TWR exchange and T_{prop} is the propagation time of the RMARKER between the devices.

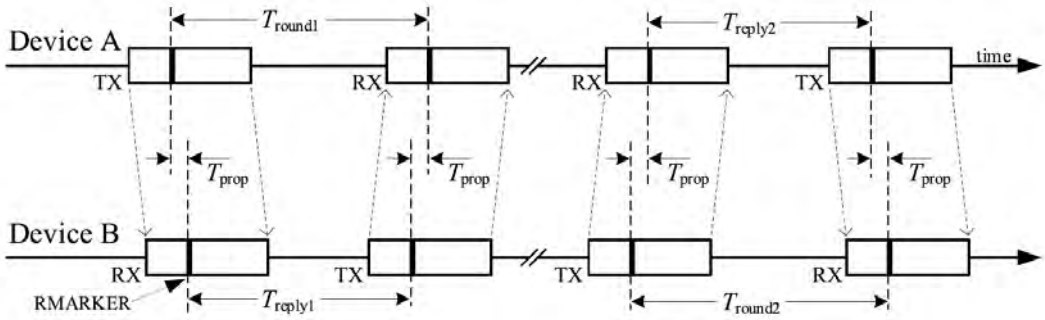


Figure 6-47b—DS-TWR

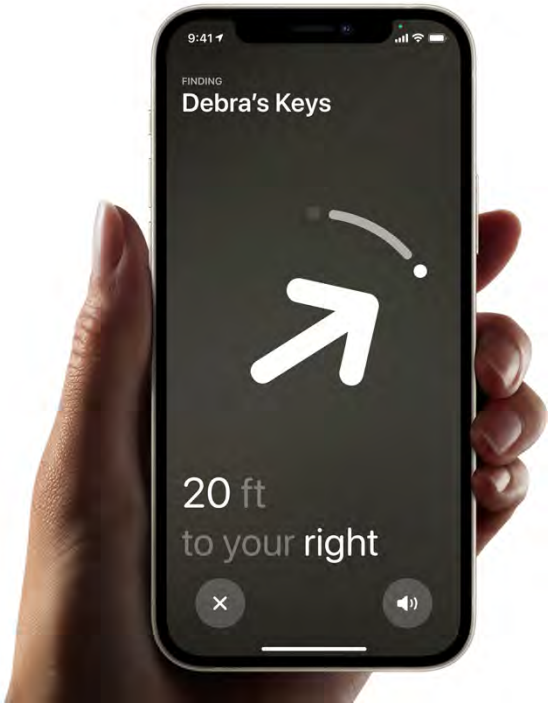
Each device precisely measures the transmission and reception times of the messages, and the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

$$\hat{T}_{prop} = \frac{(T_{round1} \times T_{round2} - T_{reply1} \times T_{reply2})}{(T_{round1} + T_{round2} + T_{reply1} + T_{reply2})}$$

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Sections 6.9.1.2.2, 6.9.1.2.3.

32. Claim 18 of the '779 Patent recites a "controller for" "estimating a range to the target wireless communications device based upon a plurality of determined propagation delays." The Accused Devices comprise a controller for estimating a range to the target wireless communications device based upon a plurality of determined propagation delays. For example, the Apple iPhone 13 comprises a controller for estimating a range to the target wireless

communications device (such as an Apple AirTag) based upon a plurality of determined propagation delays:



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

34

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

35

6.9.1.1 Overview

Support for ranging is optional. A device that supports ranging is called a ranging-capable device (RDEV). An RDEV shall support the ranging counter described in 6.9.1.3 and the figure of merit (FoM) described in 6.9.1.7. An RDEV may support optional crystal characterization described in 6.9.1.6 and the optional dynamic preamble code and channel selection (DPS) described in "Applications of IEEE Std 802.15.4" [B3]. RDEVs produce ranging results, used by higher layers to compute the ranges between devices. These ranging results may include transmit and receive ranging counter values, ranging FoM, angle of arrival (AOA) information, ranging tracking interval, and ranging tracking offset values.

~~Ranging is an optional feature.~~ This standard includes optional features to support relative positioning and localization. Accurate location may be achieved by a ranging-capable device (RDEV) using one of the ultra wideband (UWB) PHYs defined in this standard that provide the capability to accurately determine packet reception and transmission times. With accurate message timestamping, techniques such as two-way ranging (TWR) time of flight (TOF) can give very accurate estimates of relative separation distance between two devices. Similarly, an accurate location estimate for a mobile device can be determined, for example, when its distance from a number of fixed devices (of known location) is ascertained.

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Section 6.9.1.1.

33. Apple also knowingly and intentionally induces infringement of one or more claims of the '779 Patent in violation of 35 U.S.C. § 271(b). At least as of the filing and service of this amended complaint, Apple has knowledge of the '779 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '779 Patent, Apple continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '779 Patent, for example by utilizing the accused ultra-wideband functionality on the Accused Products in an infringing manner. *See, e.g.*, https://support.apple.com/en-gb/guide/iphone/ipha779f0c10/15.0/ios/15.0 (Apple iPhone 13 User Manual – "Locate an AirTag or other item in Find My on iPhone"); https://support.apple.com/en-us/HT210973 (Apple AirTag instructions). Further, Apple advertises to its customers and end users that the "Precision Finding"

mode on an Apple handset utilizes the infringing ultra-wideband technology to locate an Apple AirTag. *See* https://support.apple.com/en-gb/HT210967. Apple provides these instructions and online materials knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Apple also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '779 Patent, thereby specifically intending for and inducing its customers to infringe the '779 Patent through the customers' normal and customary use of the Accused Products.

34. Apple has also infringed, and continues to infringe, one or more claims of the '779 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '779 Patent, are especially made or adapted to infringe the '779 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use (as exemplified by the materials cited above). At least as of the filing and service of this complaint, Apple has knowledge of the '779 Patent and the infringing nature of the Accused Products. Apple has been, and currently is, contributorily infringing the '779 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

35. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Apple has injured Plaintiff and is liable for infringement of the '779 Patent pursuant to 35 U.S.C. § 271.

36. As a result of Apple's direct infringement of the '779 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

37. As a result of Apple's indirect infringement of the '779 Patent (induced and contributory), Plaintiff is entitled to monetary damages (present and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 7,321,777

38. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

39. Apple has been and is now directly infringing the '777 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products and systems, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '777 Patent, including but not limited to claim 12.

40. Claim 12 of the '777 Patent recites "[a] wireless device locator for locating a target wireless communications device." To the extent the preamble is limiting, the Accused Products comprise of a wireless device locator for locating a target wireless communications device. For example, the accused Apple iPhone 13 supports ultra-wideband functionality for locating a target wireless communications device, such as the Apple AirTag:

iPhone 13 Overview Switching to iPhone Tech Specs Buy

All models	5G (sub-6 GHz and mmWave)[7]
	Gigabit LTE with 4x4 MIMO and LAA[7]
	Wi-Fi 6 (802.11ax) with 2x2 MIMO
	Bluetooth 5.0 wireless technology
	Ultra Wideband chip for spatial awareness[8]
	NFC with reader mode
	Express Cards with power reserve

See https://www.apple.com/iphone-13/specs/.

AirTag Buy

Connectivity	Bluetooth for proximity finding
	Apple-designed U1 chip for Ultra Wideband and Precision Finding
	NFC tap for Lost Mode

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

41. Claim 12 of the '777 Patent recites that the wireless device locator comprises "at least one antenna and a transceiver connected thereto." The Accused Products comprise at least one antenna and a transceiver connected thereto. For example, the Apple iPhone 13 comprises at least one antenna and a transceiver:

iPhone 13 Overview Switching to iPhone Tech Specs Buy

All models	5G (sub-6 GHz and mmWave)[7]
	Gigabit LTE with 4x4 MIMO and LAA[7]
	Wi-Fi 6 (802.11ax) with 2x2 MIMO
	Bluetooth 5.0 wireless technology
	Ultra Wideband chip for spatial awareness[8]
	NFC with reader mode
	Express Cards with power reserve

See https://www.apple.com/iphone-13/specs/.

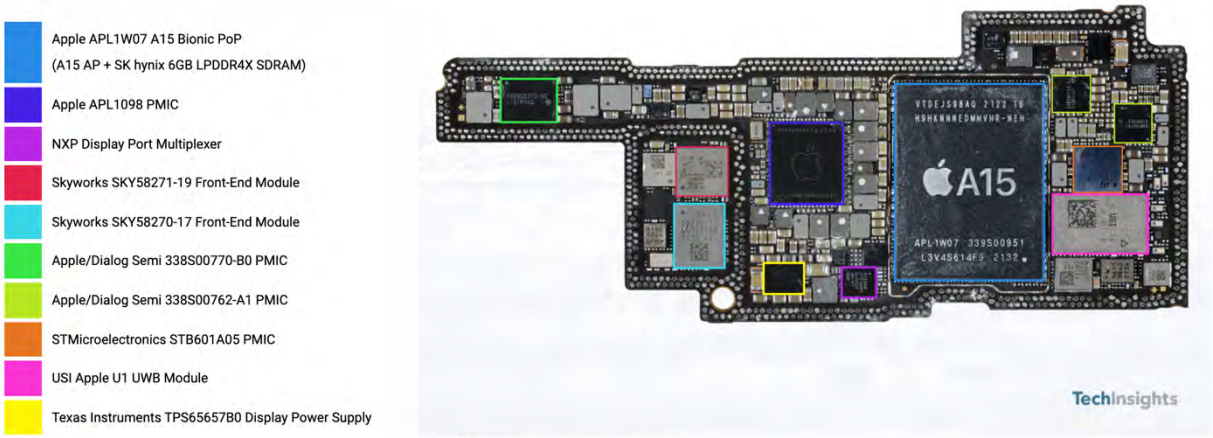


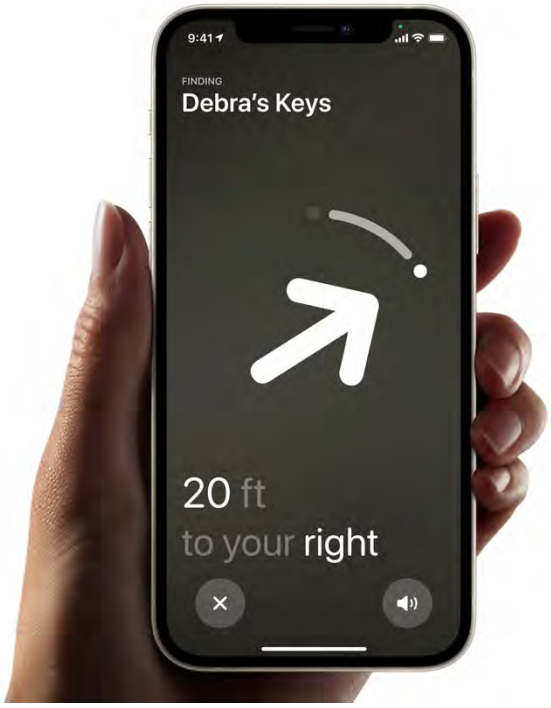
Figure 1. Apple iPhone Pro Board Shot

See https://www.techinsights.com/blog/teardown/apple-iphone-13-pro-teardown.

42. Claim 12 of the ’777 Patent recites “a controller for” “cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device and receiving a respective reply signal therefrom for each of said location finding signals.” The Accused Products comprise a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device and receiving a respective reply signal therefrom for each of said location finding signals. For example, the Apple iPhone 13 comprises a controller that cooperates with a transceiver for transmitting a plurality of location finding signals to a target wireless communications device (such

40

as the Apple AirTag) and receiving a respective reply signal therefrom for each of said location finding signals:



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

41

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

42

6.9.1.2.2 Single-sided two-way ranging (SS-TWR)

SS-TWR involves a measurement of the round-trip delay of a single message from one device to another and a response sent back to the original device. The operation of SS-TWR is as shown in Figure 6-47a, where device A initiates the exchange and device B responds to complete the exchange and T_{prop} is the propagation time of the RMARKER between the devices.

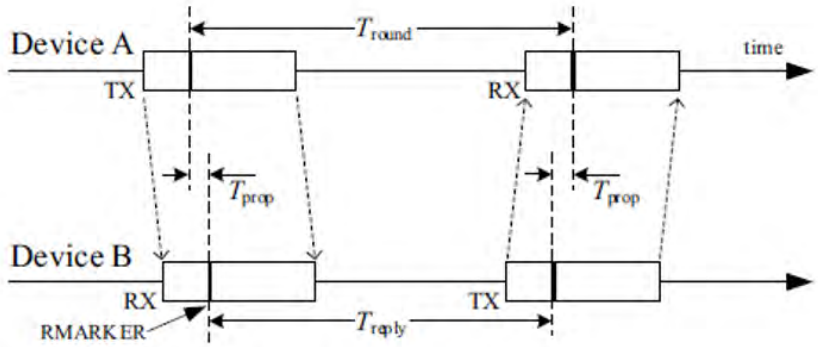


Figure 6-47a—SS-TWR

Each device precisely measures the transmission and reception times of the message frames, and so can calculate times T_{round} and T_{reply} by simple subtraction. Hence, the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

$$\hat{T}_{prop} = \frac{1}{2}(T_{round} - T_{reply})$$

* * *

When employing SS-TWR, for the TOF to be calculated at device A, device A needs the reply time T_{reply} employed by device B. When T_{reply} is determined by device B after its transmission, an additional message is necessary to bring this value to device A, as shown in Figure 6-48a and described in 6.9.6.3. When T_{reply} can be accurately predicted by device B before its transmission, the value can be embedded in the reply message itself, as shown in Figure 6-48b and described in 6.9.6.4. Alternatively, if device B has the ability to always reply with sufficiently accurate constant or pre-known reply time, it obviates the need for any transfer of T_{reply} as part of the ranging exchange, as described in 6.9.6.5.

* * *

43

6.9.1.2.3 Double-sided two-way ranging (DS-TWR)

DS-TWR is an extension of SS-TWR in which two round-trip time measurements are used and combined to give the TOF result with a reduced error in the presence of uncorrected clock frequency offset even for quite long response delays. The operation of DS-TWR is shown in Figure 6-47b, where device A initiates the first round-trip time measurement to which device B responds, after which device B initiates the second round-trip time measurement to which device A responds completing the full DS-TWR exchange and T_{prop} is the propagation time of the RMARKER between the devices.

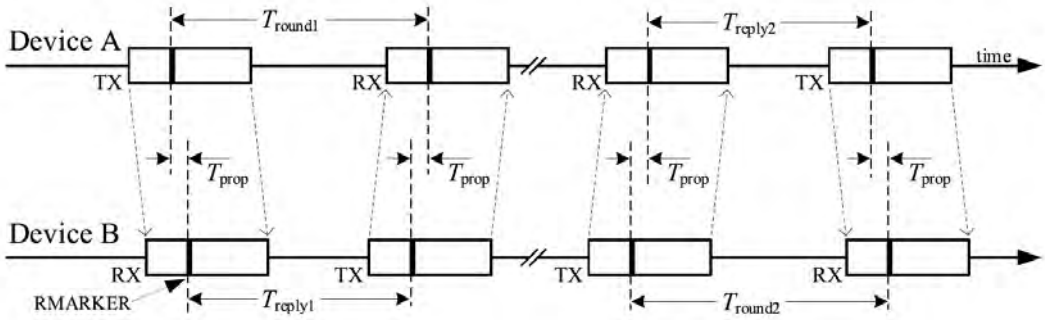


Figure 6-47b—DS-TWR

Each device precisely measures the transmission and reception times of the messages, and the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

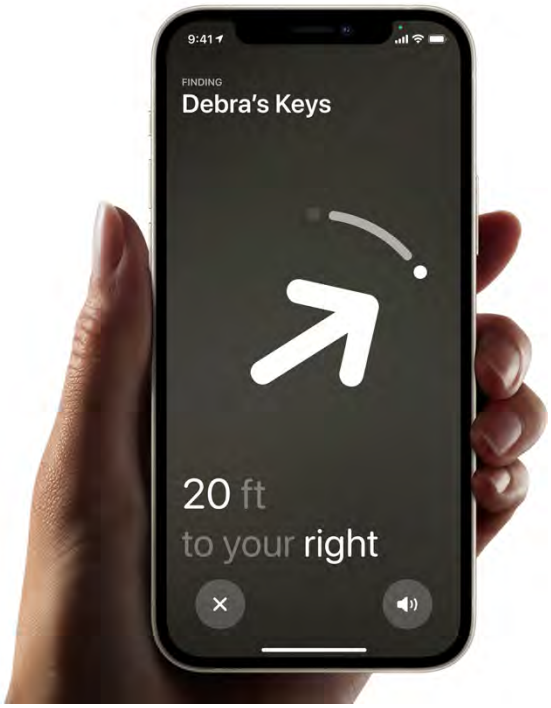
$$\hat{T}_{prop} = \frac{(T_{round1} \times T_{round2} - T_{reply1} \times T_{reply2})}{(T_{round1} + T_{round2} + T_{reply1} + T_{reply2})}$$

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Sections 6.9.1.2.2, 6.9.1.2.3.

43. Claim 12 of the '777 Patent recites "a controller for" "determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device." The Accused Products comprise a controller for determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device. For example, the Apple

44

iPhone 13 comprises a controller for determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device (such as an Apple AirTag):



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

46

6.9.1.2.2 Single-sided two-way ranging (SS-TWR)

SS-TWR involves a measurement of the round-trip delay of a single message from one device to another and a response sent back to the original device. The operation of SS-TWR is as shown in Figure 6-47a, where device A initiates the exchange and device B responds to complete the exchange and T_{prop} is the propagation time of the RMARKER between the devices.

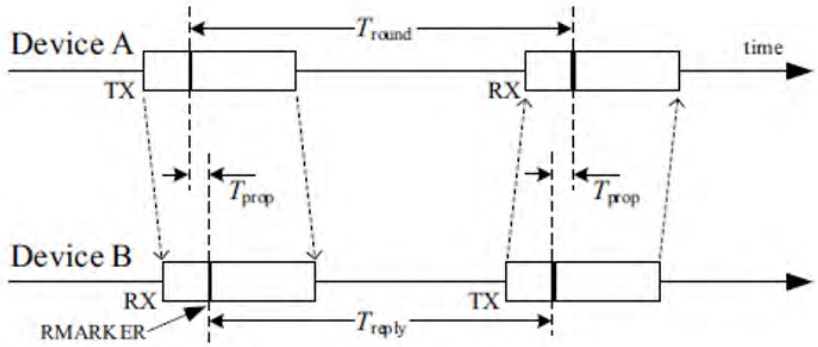


Figure 6-47a—SS-TWR

Each device precisely measures the transmission and reception times of the message frames, and so can calculate times T_{round} and T_{reply} by simple subtraction. Hence, the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

$$\hat{T}_{prop} = \frac{1}{2}(T_{round} - T_{reply})$$

* * *

When employing SS-TWR, for the TOF to be calculated at device A, device A needs the reply time T_{reply} employed by device B. When T_{reply} is determined by device B after its transmission, an additional message is necessary to bring this value to device A, as shown in Figure 6-48a and described in 6.9.6.3. When T_{reply} can be accurately predicted by device B before its transmission, the value can be embedded in the reply message itself, as shown in Figure 6-48b and described in 6.9.6.4. Alternatively, if device B has the ability to always reply with sufficiently accurate constant or pre-known reply time, it obviates the need for any transfer of T_{reply} as part of the ranging exchange, as described in 6.9.6.5.

* * *

47

6.9.1.2.3 Double-sided two-way ranging (DS-TWR)

DS-TWR is an extension of SS-TWR in which two round-trip time measurements are used and combined to give the TOF result with a reduced error in the presence of uncorrected clock frequency offset even for quite long response delays. The operation of DS-TWR is shown in Figure 6-47b, where device A initiates the first round-trip time measurement to which device B responds, after which device B initiates the second round-trip time measurement to which device A responds completing the full DS-TWR exchange and T_{prop} is the propagation time of the RMARKER between the devices.

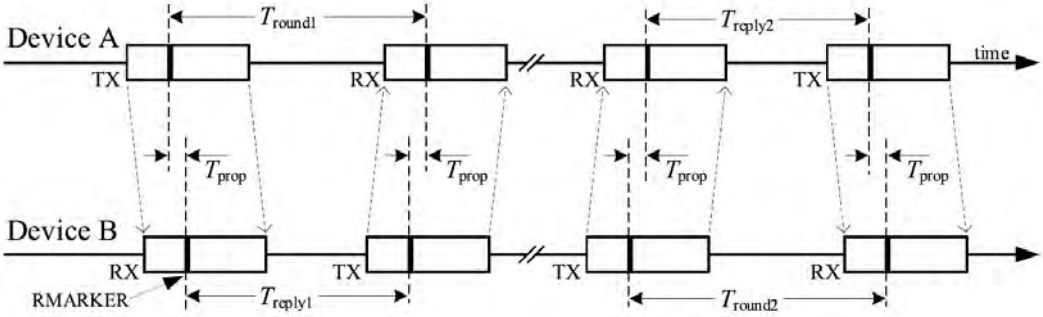


Figure 6-47b—DS-TWR

Each device precisely measures the transmission and reception times of the messages, and the resultant TOF may be estimated as $\hat{T}_{prop}$ by the equation:

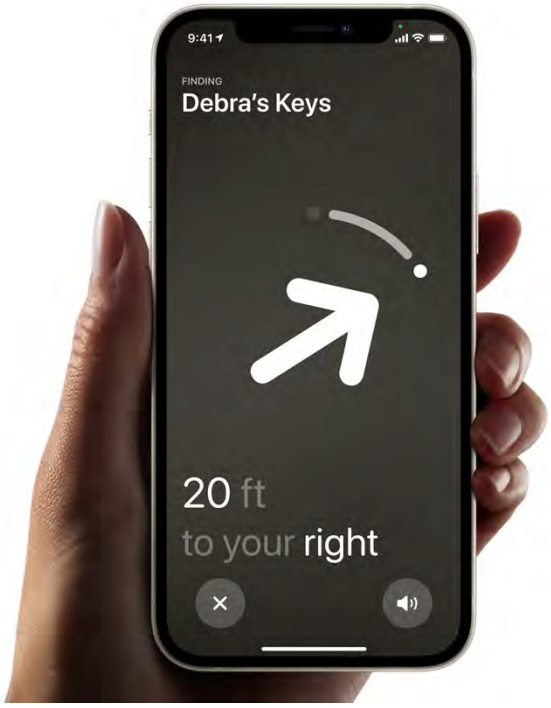
$$\hat{T}_{prop} = \frac{(T_{round1} \times T_{round2} - T_{reply1} \times T_{reply2})}{(T_{round1} + T_{round2} + T_{reply1} + T_{reply2})}$$

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Sections 6.9.1.2.2, 6.9.1.2.3.

44. Claim 12 of the '777 Patent recites "a controller for" "estimating a range to the target wireless communications device based upon a plurality of determined propagation delays." The Accused Products comprise a controller for estimating a range to the target wireless communications device based upon a plurality of determined propagation delays. For example, the Apple iPhone 13 comprises a controller for estimating a range to the target wireless

48

communications device (such as an Apple AirTag) based upon a plurality of determined propagation delays:



Cold. Warm. Warmer. Hot.

If your AirTag is nearby, your iPhone can lead you straight to it with Precision Finding.[1] You'll see the distance to your AirTag and the direction to head in — all thanks to Ultra Wideband technology.

Precision Finding compatible with:

iPhone 11
iPhone 11 Pro and iPhone 11 Pro Max
iPhone 12 and iPhone 12 mini
iPhone 12 Pro and iPhone 12 Pro Max
iPhone 13 and iPhone 13 mini
iPhone 13 Pro and iPhone 13 Pro Max

See https://www.apple.com/airtag/?afid=p238%7Cs43Yu6bTM-dc_mtid_1870765e38482_pcrid_573879837530_pgrid_120928559493_&cid=aos-us-kwgo-btb--slid---product-.

49

Use Precision Finding to pinpoint the location of your item

If you have a supported iPhone model with Ultra Wideband and your AirTag is nearby[1], you can use Precision Finding to help find it, even if it's stuck between couch cushions or hiding under a stack of mail. If your AirTag is out of range of your connected device, get directions to it first.

1. Open the Find My app, then tap the Items tab.
2. Choose the AirTag you want to locate, then tap Find. [1]
3. Follow the onscreen instructions and move around the space until your iPhone connects to your AirTag.
4. Your iPhone displays the distance and direction to your AirTag. Use that information to get closer to your AirTag until you find your lost item.
5. Tap the X button when you're done.

If you need more help

You can tap the sound button to play a sound on your AirTag if it's within Bluetooth range of your connected device. If it's too dark, a flashlight button will appear. To turn on the flashlight, tap it.

If you don't see Find, make sure that you turned on Location Access for the Find My app.

1. Go to Settings > Privacy > Location Services, and check that Location Services is on.
2. Scroll down and tap Find My.
3. Check "Ask Next Time," "While Using the App," or "While Using the App or Widgets." For the most accurate location, turn on Precise Location.

See https://support.apple.com/en-us/HT210967.

50

6.9.1.1 Overview

Support for ranging is optional. A device that supports ranging is called a ranging-capable device (RDEV). An RDEV shall support the ranging counter described in 6.9.1.3 and the figure of merit (FoM) described in 6.9.1.7. An RDEV may support optional crystal characterization described in 6.9.1.6 and the optional dynamic preamble code and channel selection (DPS) described in "Applications of IEEE Std 802.15.4" [B3]. RDEVs produce ranging results, used by higher layers to compute the ranges between devices. These ranging results may include transmit and receive ranging counter values, ranging FoM, angle of arrival (AOA) information, ranging tracking interval, and ranging tracking offset values.

~~Ranging is an optional feature.~~ This standard includes optional features to support relative positioning and localization. Accurate location may be achieved by a ranging-capable device (RDEV) using one of the ultra wideband (UWB) PHYs defined in this standard that provide the capability to accurately determine packet reception and transmission times. With accurate message timestamping, techniques such as two-way ranging (TWR) time of flight (TOF) can give very accurate estimates of relative separation distance between two devices. Similarly, an accurate location estimate for a mobile device can be determined, for example, when its distance from a number of fixed devices (of known location) is ascertained.

See IEEE 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques at Section 6.9.1.1.

45. Apple also knowingly and intentionally induces infringement of one or more claims of the '777 Patent in violation of 35 U.S.C. § 271(b). At least as of the filing and service of this amended complaint, Apple has knowledge of the '777 Patent and the infringing nature of the Accused Products. For example, Apple obtained knowledge of the '777 Patent at least as of January 21, 2022 when it was served with the initial complaint. Dkt. No. 6. Despite this knowledge of the '777 Patent, Apple continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '777 Patent, for example by utilizing the accused ultra-wideband functionality on the Accused Products in an infringing manner. *See, e.g.*, https://support.apple.com/en-gb/guide/iphone/ipha779f0c10/15.0/ios/15.0 (Apple iPhone 13 User Manual – "Locate an AirTag or other item in Find My on iPhone");

https://support.apple.com/en-us/HT210973 (Apple AirTag instructions). Further, Apple advertises to its customers and end users that the "Precision Finding" mode on an Apple handset utilizes the infringing ultra-wideband technology to locate an Apple AirTag. *See* https://support.apple.com/en-gb/HT210967. Apple provides these instructions and online materials knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Apple also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '777 Patent, thereby specifically intending for and inducing its customers to infringe the '777 Patent through the customers' normal and customary use of the Accused Products.

46. Apple has also infringed, and continues to infringe, one or more claims of the '777 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '777 Patent, are especially made or adapted to infringe the '777 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use (as exemplified by the materials cited above). At least as of the filing and service of this amended complaint, Apple has knowledge of the '777 Patent and the infringing nature of the Accused Products. Apple has been, and currently is, contributorily infringing the '777 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

47. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Apple has injured Plaintiff and is liable for infringement of the '777 Patent pursuant to 35 U.S.C. § 271.

48. As a result of Apple's direct infringement of the '777 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Apple's

infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

49. As a result of Apple's indirect infringement of the '777 Patent (induced and contributory), Plaintiff is entitled to monetary damages (present and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 7,765,399

50. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

51. Apple has been and is now directly infringing the '399 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '399 Patent, including but not limited to claim 1.

52. Claim 1 of the '399 Patent recites "[a] computer system, comprising: a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine." The Accused Products comprise a computer system comprising a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine. For example, the iPhone 13 is a computer system comprising a portable mobile computing device that includes a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine:

iPhone 13

Overview | Switching to iPhone | Tech Specs | Buy

All models	5G (sub-6 GHz and mmWave)[7]
	Gigabit LTE with 4x4 MIMO and LAA[7]
	Wi-Fi 6 (802.11ax) with 2x2 MIMO
	Bluetooth 5.0 wireless technology
	Ultra Wideband chip for spatial awareness[8]
	NFC with reader mode
	Express Cards with power reserve

See https://www.apple.com/iphone-13/specs/.

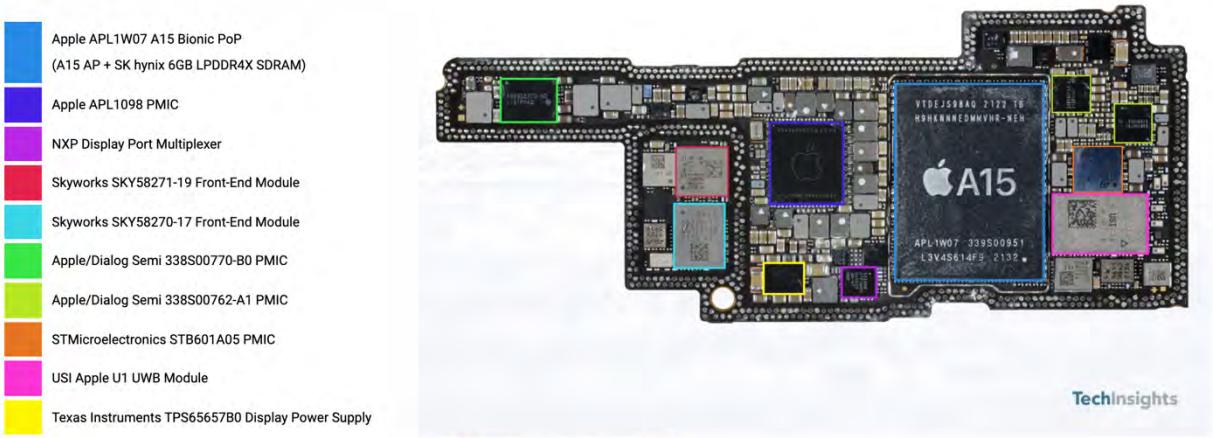


Figure 1. Apple iPhone Pro Board Shot

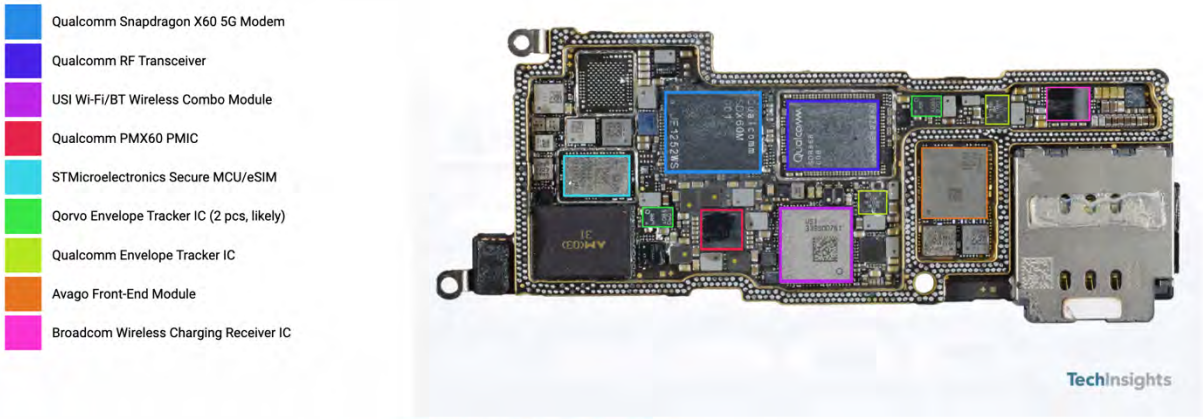
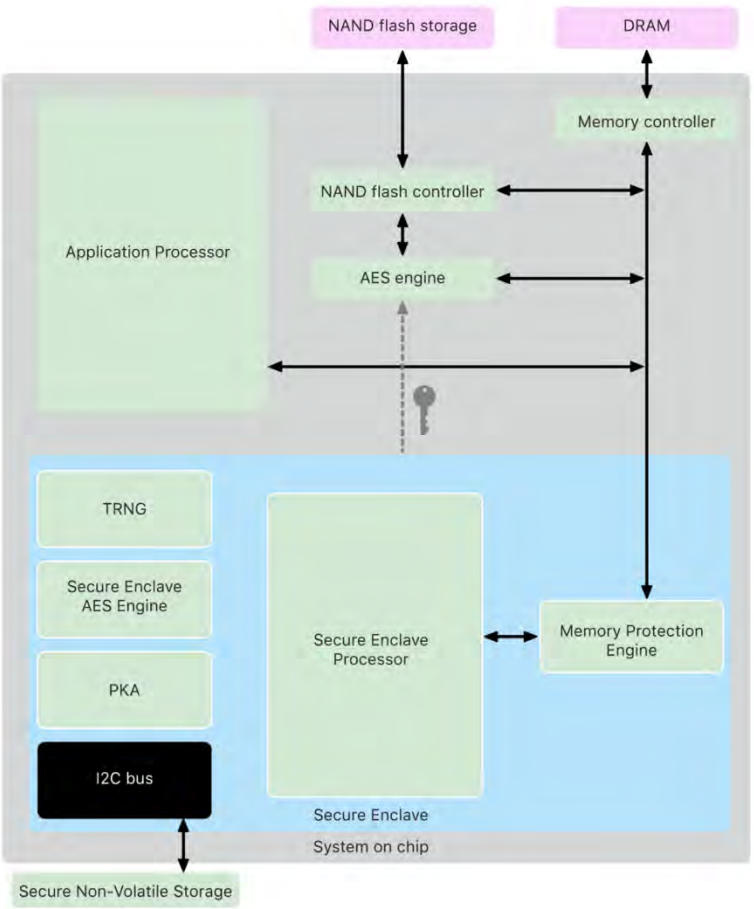


Figure 3. Apple iPhone Pro Board Shot

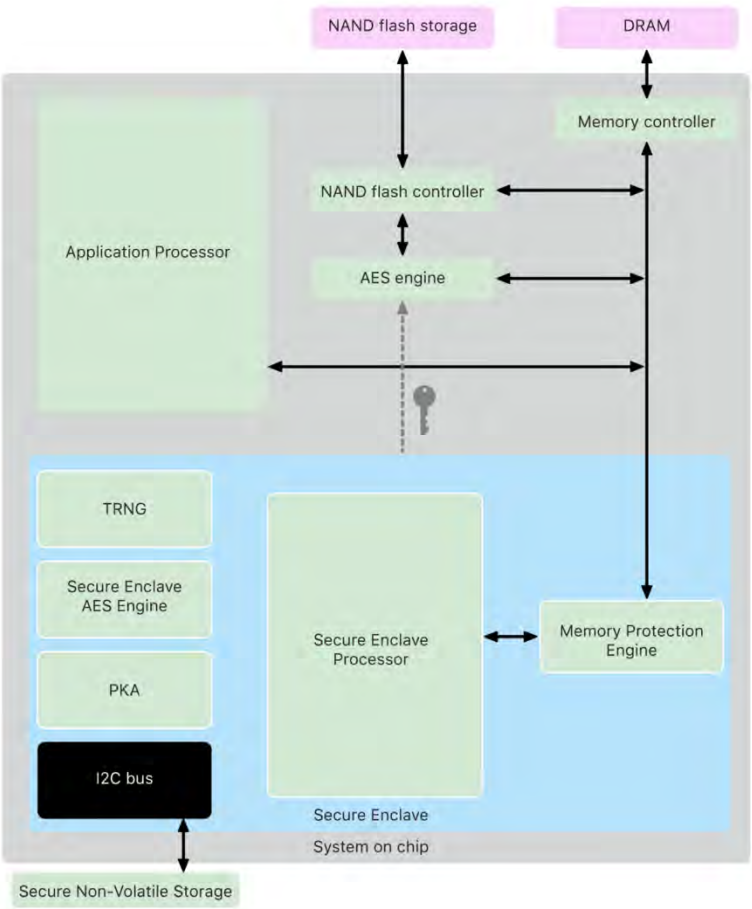
See https://www.techinsights.com/blog/teardown/apple-iphone-13-pro-teardown.

54



See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

53. Claim 1 recites "said secure user processor comprising" "a trusted microprocessor, a trusted operating system executing on said trusted microprocessor, and a trusted application software executing on said trusted microprocessor." The Accused Products comprise a secure user processor comprising a trusted microprocessor, a trusted operating system executing on said trusted microprocessor, and a trusted application software executing on said trusted microprocessor. For example, the iPhone 13 contains a Secure Enclave Processor with a trusted microprocessor, a trusted operating system executing on the trusted microprocessor, and a trusted application software executing on the trusted microprocessor:



Secure Enclave Processor

The Secure Enclave Processor provides the main computing power for the Secure Enclave. To provide the strongest isolation, the Secure Enclave Processor is dedicated solely for Secure Enclave use. This helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

The Secure Enclave Processor runs an Apple-customised version of the L4 microkernel. It's designed to operate efficiently at a lower clock speed that helps protect it against clock and power attacks. The Secure Enclave Processor, starting with the A11 and S4, includes a memory-protected engine and encrypted memory with anti-replay capabilities, secure boot, a dedicated random number generator and its own AES engine.

56

Secure Enclave Boot ROM

The Secure Enclave includes a dedicated Secure Enclave Boot ROM. Like the Application Processor Boot ROM, the Secure Enclave Boot ROM is immutable code that establishes the hardware root of trust for the Secure Enclave.

On system startup, iBoot assigns a dedicated region of memory to the Secure Enclave. Before using the memory, the Secure Enclave Boot ROM initialises the Memory Protection Engine to provide cryptographic protection of the Secure Enclave protected memory.

The Application Processor then sends the sepOS image to the Secure Enclave Boot ROM. After copying the sepOS image into the Secure Enclave protected memory, the Secure Enclave Boot ROM checks the cryptographic hash and signature of the image to verify that the sepOS is authorised to run on the device. If the sepOS image is properly signed to run on the device, the Secure Enclave Boot ROM transfers control to sepOS. If the signature isn't valid, the Secure Enclave Boot ROM is designed to prevent any further use of the Secure Enclave until the next chip reset.

On Apple A10 and later SoCs, the Secure Enclave Boot ROM locks a hash of the sepOS into a register dedicated to this purpose. The Public Key Accelerator uses this hash for operating-system-bound (OS-bound) keys.

See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

54. Claim 1 recites "said non-secure user processor comprising" "an untrusted microprocessor, an untrusted operating system executing on said untrusted microprocessor, and an untrusted application software executing on said untrusted microprocessor." The Accused Products comprise a non-secure user processor comprising an untrusted microprocessor, an untrusted operating system executing on said untrusted microprocessor, and an untrusted application software executing on said untrusted microprocessor. For example, the iPhone 13 comprises an Application Processor comprising an untrusted microprocessor, an untrusted operating system executing on the untrusted microprocessor, and untrusted application software executing on the untrusted microprocessor:

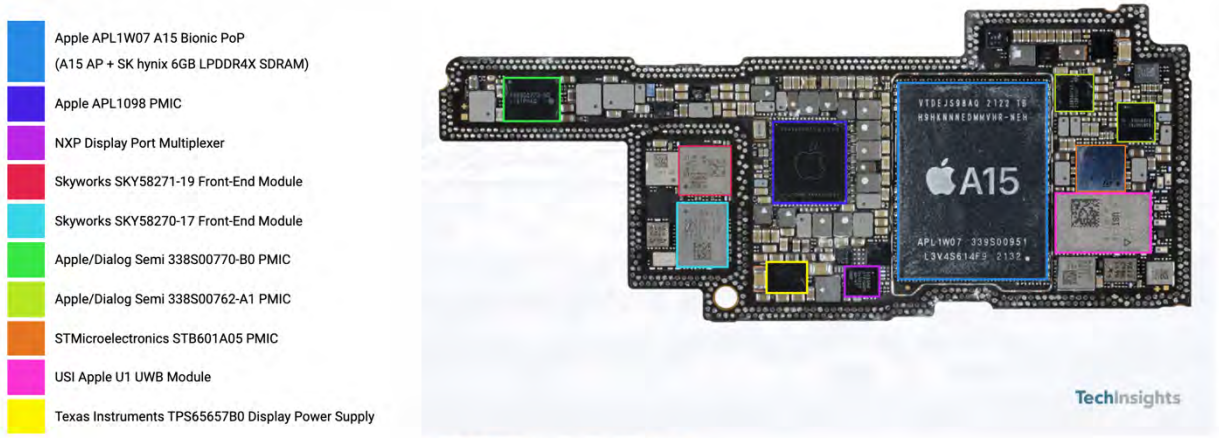
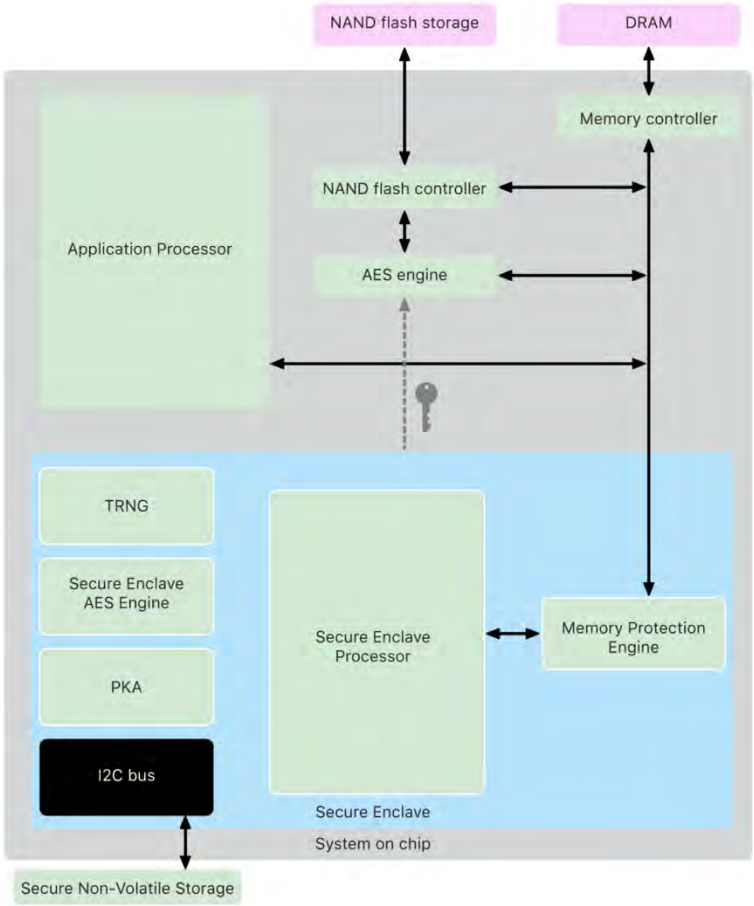


Figure 1. Apple iPhone Pro Board Shot

See https://www.techinsights.com/blog/teardown/apple-iphone-13-pro-teardown.

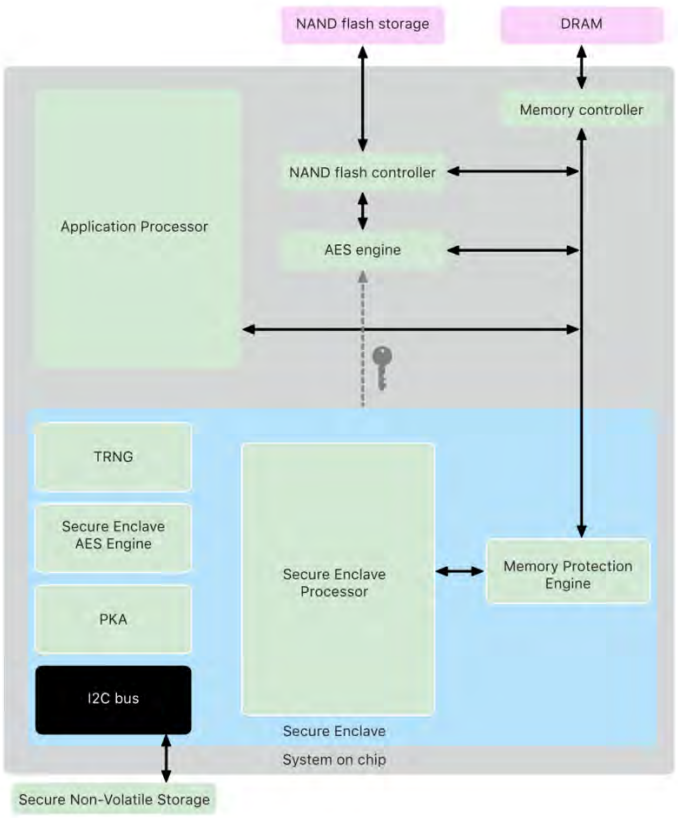


See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

iOS 15 is packed with new features that help you connect with others, be more present and in the moment, explore the world, and use powerful intelligence to do more with iPhone than ever before.

See https://www.apple.com/ios/ios-15/.

55. Claim 1 recites "said cryptographic engine configured for encrypting any data communicated from said secure user processor to said non-secure user processor, comprising" "a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptographic processor." The Accused Products comprise a cryptographic engine configured for encrypting data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor and a trusted operating system executing on the trusted cryptographic processor. For example, the iPhone 13 contains a Secure Enclave AES Engine and a trusted operating system:



59

Secure Enclave Processor

The Secure Enclave Processor provides the main computing power for the Secure Enclave. To provide the strongest isolation, the Secure Enclave Processor is dedicated solely for Secure Enclave use. This helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

The Secure Enclave Processor runs an Apple-customised version of the L4 microkernel. It's designed to operate efficiently at a lower clock speed that helps protect it against clock and power attacks. The Secure Enclave Processor, starting with the A11 and S4, includes a memory-protected engine and encrypted memory with anti-replay capabilities, secure boot, a dedicated random number generator and its own AES engine.

Secure Enclave AES Engine

The Secure Enclave AES Engine is a hardware block used to perform symmetric cryptography based on the AES cipher. The AES Engine is designed to resist leaking information by using timing and Static Power Analysis (SPA). Starting with the A9 SoC, the AES Engine also includes Dynamic Power Analysis (DPA) countermeasures.

The AES Engine supports hardware and software keys. Hardware keys are derived from the Secure Enclave UID or GID. These keys stay within the AES Engine and aren't made visible even to sepOS software. Although software can request encryption and decryption operations with hardware keys, it can't extract the keys.

On Apple A10 and newer SoCs, the AES Engine includes lockable seed bits that diversify keys derived from the UID or GID. This allows data access to be conditioned on the device's mode of operation. For example, lockable seed bits are used to deny access to password-protected data when booting from Device Firmware Update (DFU) mode. For more information, see Passcodes and passwords.

See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

56. Claim 1 recites "a first data communication link communicating data between said secure processor and said cryptographic engine." The Accused Products comprise a first data communication link communicating data between said secure processor and said cryptographic engine. For example, the iPhone 13 contains a Secure Enclave Processor that contains a data communication link that communicates data between the Secure Enclave Processor to the AES Engine:

Secure Enclave Processor

The Secure Enclave Processor provides the main computing power for the Secure Enclave. To provide the strongest isolation, the Secure Enclave Processor is dedicated solely for Secure Enclave use. This helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

The Secure Enclave Processor runs an Apple-customised version of the L4 microkernel. It's designed to operate efficiently at a lower clock speed that helps protect it against clock and power attacks. The Secure Enclave Processor, starting with the A11 and S4, includes a memory-protected engine and encrypted memory with anti-replay capabilities, secure boot, a dedicated random number generator and its own AES engine.

Secure Enclave AES Engine

The Secure Enclave AES Engine is a hardware block used to perform symmetric cryptography based on the AES cipher. The AES Engine is designed to resist leaking information by using timing and Static Power Analysis (SPA). Starting with the A9 SoC, the AES Engine also includes Dynamic Power Analysis (DPA) countermeasures.

The AES Engine supports hardware and software keys. Hardware keys are derived from the Secure Enclave UID or GID. These keys stay within the AES Engine and aren't made visible even to sepOS software. Although software can request encryption and decryption operations with hardware keys, it can't extract the keys.

On Apple A10 and newer SoCs, the AES Engine includes lockable seed bits that diversify keys derived from the UID or GID. This allows data access to be conditioned on the device's mode of operation. For example, lockable seed bits are used to deny access to password-protected data when booting from Device Firmware Update (DFU) mode. For more information, see Passcodes and passwords.

See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

57. Claim 1 recites "a second data communication link communicating data between said non-secure processor and said cryptographic engine." The Accused Products comprise a second data communication link communicating data between said non-secure processor and said cryptographic engine. For example, the iPhone 13 contains a data communication link between the Application Processor and the Secure Enclave AES Engine:

61

Secure Enclave AES Engine

The Secure Enclave AES Engine is a hardware block used to perform symmetric cryptography based on the AES cipher. The AES Engine is designed to resist leaking information by using timing and Static Power Analysis (SPA). Starting with the A9 SoC, the AES Engine also includes Dynamic Power Analysis (DPA) countermeasures.

The AES Engine supports hardware and software keys. Hardware keys are derived from the Secure Enclave UID or GID. These keys stay within the AES Engine and aren't made visible even to sepOS software. Although software can request encryption and decryption operations with hardware keys, it can't extract the keys.

On Apple A10 and newer SoCs, the AES Engine includes lockable seed bits that diversify keys derived from the UID or GID. This allows data access to be conditioned on the device's mode of operation. For example, lockable seed bits are used to deny access to password-protected data when booting from Device Firmware Update (DFU) mode. For more information, see Passcodes and passwords.

Secure Enclave Boot ROM

The Secure Enclave includes a dedicated Secure Enclave Boot ROM. Like the Application Processor Boot ROM, the Secure Enclave Boot ROM is immutable code that establishes the hardware root of trust for the Secure Enclave.

On system startup, iBoot assigns a dedicated region of memory to the Secure Enclave. Before using the memory, the Secure Enclave Boot ROM initialises the Memory Protection Engine to provide cryptographic protection of the Secure Enclave protected memory.

The Application Processor then sends the sepOS image to the Secure Enclave Boot ROM. After copying the sepOS image into the Secure Enclave protected memory, the Secure Enclave Boot ROM checks the cryptographic hash and signature of the image to verify that the sepOS is authorised to run on the device. If the sepOS image is properly signed to run on the device, the Secure Enclave Boot ROM transfers control to sepOS. If the signature isn't valid, the Secure Enclave Boot ROM is designed to prevent any further use of the Secure Enclave until the next chip reset.

On Apple A10 and later SoCs, the Secure Enclave Boot ROM locks a hash of the sepOS into a register dedicated to this purpose. The Public Key Accelerator uses this hash for operating-system-bound (OS-bound) keys.

See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.

58. Claim 1 recites "a secure human/machine interface configured for enabling bi-directional communication of classified information exclusively between a user and said secure user processor." The Accused Products comprise a secure human/machine interface configured for enabling bi-directional communication of classified information exclusively between a user

and said secure user processor. For example, the iPhone 13 contains FaceID, which enables bi-directional communication of classified information exclusively between a user and the Secure Enclave Processor. For example, other Accused Products contain TouchID, which enables bi-directional communication of classified information between a user and the Secure Enclave Processor.

Touch ID and Face ID security

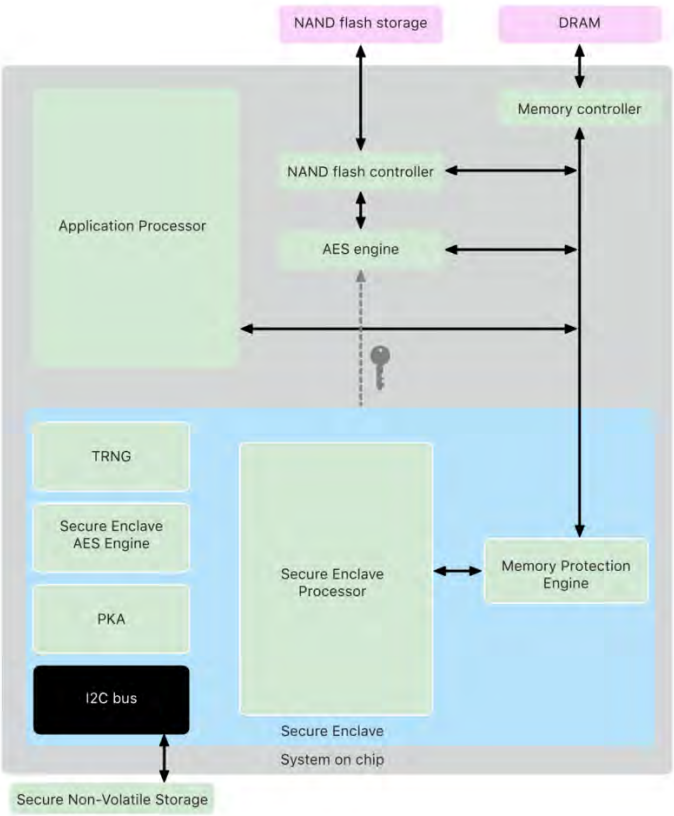
Passcodes and passwords are essential to the security of Apple devices. At the same time, users require convenient access to their devices, often more than a hundred times a day. Biometric authentication provides a way to retain the security of a strong passcode — or even strengthen the passcode or password because it need not be entered manually — while providing the convenience of swiftly unlocking with a finger press or glance. Touch ID and Face ID don't replace a passcode or password, but in most situations they do make access faster and easier.

Apple's biometric security architecture relies on a strict separation of responsibilities between the biometric sensor and the Secure Enclave, and a secure connection between the two. The sensor captures the biometric image and securely transmits it to the Secure Enclave. During enrolment, the Secure Enclave processes, encrypts and stores the corresponding Touch ID and Face ID template data. During matching, the Secure Enclave compares incoming data from the biometric sensor against the stored templates to determine whether to unlock the device or respond that a match is valid (for Apple Pay, in-app and other uses of Touch ID and Face ID). The architecture supports devices that include both the sensor and Secure Enclave (such as iPhone, iPad and many Mac systems), as well as the ability to physically separate the sensor into a peripheral that is then securely paired to the Secure Enclave in a Mac with Apple silicon.

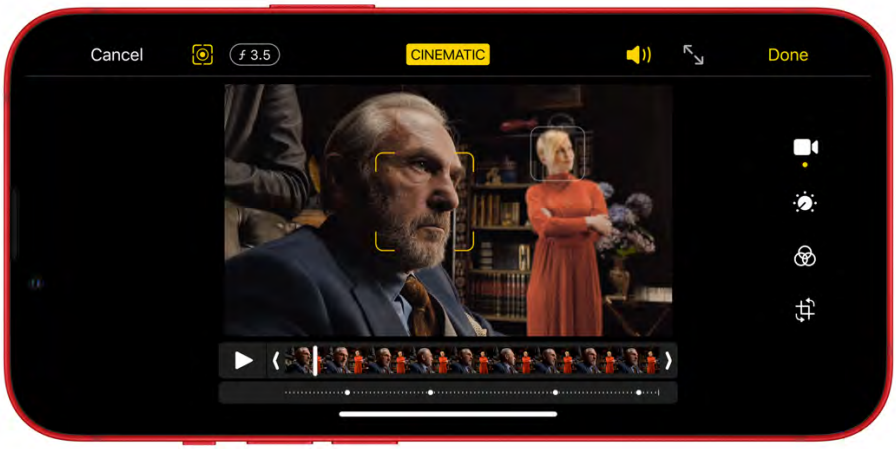
See https://support.apple.com/en-in/guide/security/sec067eb0c9e/web.

59. Claim 1 recites "a non-secure human/machine interface distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure user processor." The Accused Products comprise a non-secure human/machine interface distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure user processor. For example, the iPhone 13 contains a touchscreen and related software/hardware that enables bi-

directional communication of unclassified information between the user and the Application Processor:



See https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web.



See https://www.apple.com/iphone-13/.

64

Both models:

HDR display
True Tone
Wide color (P3)
Haptic Touch
2,000,000:1 contrast ratio (typical)
800 nits max brightness (typical); 1200 nits max brightness (HDR)
Fingerprint-resistant oleophobic coating
Support for display of multiple languages and characters simultaneously

See https://www.apple.com/iphone-13/specs/.

60. Claim 1 recites "wherein said communications transceiver is operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device." The Accused Products comprise a communication transceiver that is operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device. For example, the iPhone 13 comprises a communication transceiver operatively coupled to the Application Processor and configured for communicating data to other devices:

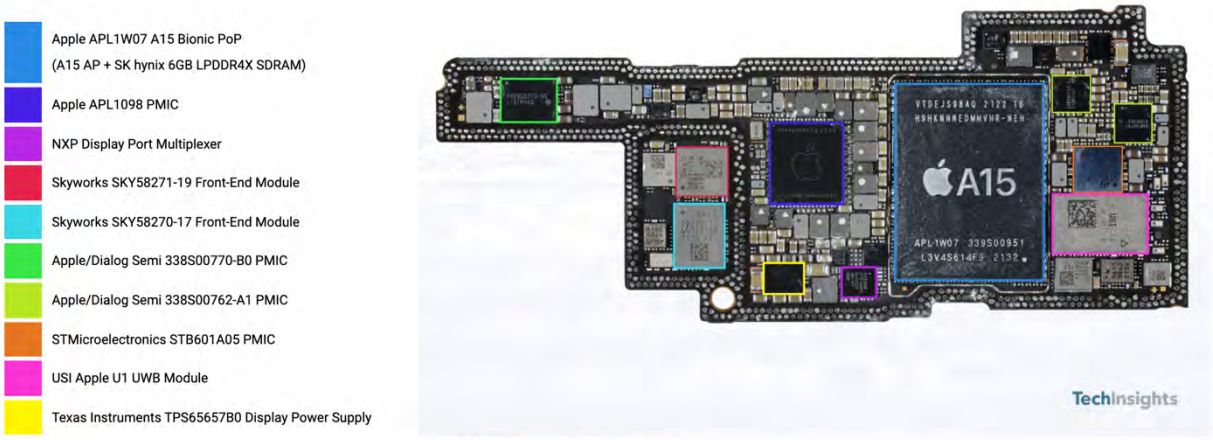


Figure 1. Apple iPhone Pro Board Shot

65

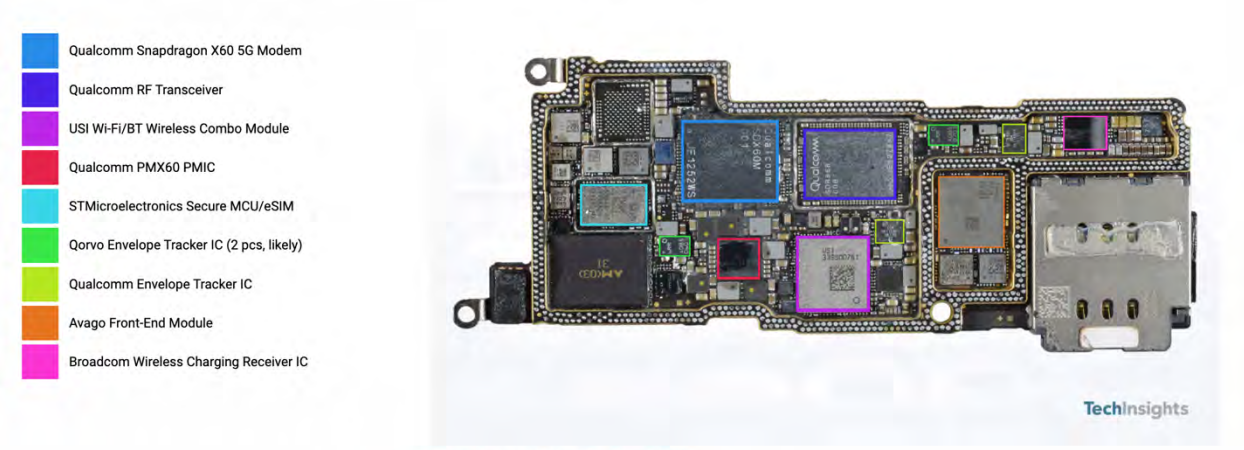


Figure 3. Apple iPhone Pro Board Shot

See https://www.techinsights.com/blog/teardown/apple-iphone-13-pro-teardown.

61. Apple also knowingly and intentionally induces infringement of one or more claims of the '399 Patent in violation of 35 U.S.C. § 271(b). At least as of the filing and service of this amended complaint, Apple has knowledge of the '399 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '399 Patent, Apple continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '399 Patent, for example by utilizing the Secure Enclave Processor on the Accused Products in an infringing manner. *See, e.g.*, https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web (Apple Platform Security – Secure Enclave); https://support.apple.com/en-gb/guide/iphone/ipha779f0c10/15.0/ios/15.0 (Apple iPhone 13 User Manual – "Use the built-in security and privacy protection of iPhone"). Further, Apple advertises to its customers and end users that the iPhone 13 uses the Application Processor and Secure Enclave Processor for an enhanced user experience that also protects personal information. *See, e.g.*, https://www.apple.com/iphone-13/. Apple further advertises and instructs its users on using TouchID and FaceID. *See, e.g.*, https://support.apple.com/en-

in/guide/security/secc5227ff3c/1/web/1 ("Uses for Touch ID and Face ID"). Apple provides these instructions and online materials knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Apple also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '399 Patent, thereby specifically intending for and inducing its customers to infringe the '399 Patent through the customers' normal and customary use of the Accused Products.

62. Apple has also infringed, and continues to infringe, one or more claims of the '399 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '399 Patent, are especially made or adapted to infringe the '399 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use (as exemplified by the materials cited above). At least as of the filing and service of this amended complaint, Apple has knowledge of the '399 Patent and the infringing nature of the Accused Products. Apple has been, and currently is, contributorily infringing the '399 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

63. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Apple has injured Plaintiff and is liable for infringement of the '399 Patent pursuant to 35 U.S.C. § 271.

64. As a result of Apple's direct infringement of the '399 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

65. As a result of Apple's indirect infringement of the '399 Patent (induced and contributory), Plaintiff is entitled to monetary damages (present and future) in an amount adequate

to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple, together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Apple has infringed, either literally and/or under the doctrine of equivalents, the '780, '779, '777, and '399 Patents;

b. A judgment and order requiring Apple to pay Plaintiff its damages (past, present, and future), costs, expenses, and pre-judgment and post-judgment interest for Apple's infringement of the '780, '779, '777, and '399 Patents;

c. A judgment and order requiring Apple to pay Plaintiff compulsory ongoing licensing fees, as determined by the Court in equity.

d. A judgment and order requiring Apple to provide an accounting and to pay supplemental damages to Plaintiff, including without limitation, pre-judgment and post-judgment interest and compensation for infringing products released after the filing of this case that are not colorably different from the accused products;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Apple; and

f. Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: March 22, 2022

Respectfully submitted,

/s/Brett Cooper

Brett E. Cooper (NY SBN 4011011) (Lead Counsel)
bcooper@raklaw.com
Reza Mirzaie (CA SBN 246953)
rmirzaie@raklaw.com
Marc A. Fenster (CA SBN 181067)
mfenster@raklaw.com
Seth Hasenour (TX SBN 24059910)
shasenour@raklaw.com
Drew B. Hollander (NY SBN 5378096)
dhollander@raklaw.com

RUSS AUGUST & KABAT
12424 Wilshire Blvd. 12th Floor
Los Angeles, CA 90025
Phone: (310) 826-7474
Facsimile: (310) 826-6991

Attorneys for Plaintiff Speir Technologies Limited

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record are being served with a copy of the foregoing document via the Court's CM/ECF system on March 22, 2022

/s/ Brett E. Cooper
Brett E. Cooper

70

Exhibit 1

US008345780B2

(12) **United States Patent**
Chauncey et al.

(10) **Patent No.: US 8,345,780 B2**
(45) **Date of Patent: Jan. 1, 2013**

(54) **WIRELESS COMMUNICATION SYSTEM COMPENSATING FOR INTERFERENCE AND RELATED METHODS**

(75) Inventors: **David Chauncey**, Fairport, NY (US); **Mitel Kuliner**, Rochester, NY (US); **Elias Theodorou**, Rochester, NY (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1246 days.

(21) Appl. No.: **12/132,757**

(22) Filed: **Jun. 4, 2008**

(65) **Prior Publication Data**

US 2009/0304095 A1 Dec. 10, 2009

(51) **Int. Cl.**
H04K 1/10 (2006.01)

(52) **U.S. Cl.** **375/260**; 375/259; 375/219; 375/295; 375/316; 375/346; 375/350; 370/328; 370/335; 370/342; 370/310

(58) **Field of Classification Search** 375/260, 375/259, 219, 295, 316, 346, 350; 370/328, 370/335, 342, 310
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,115,409	A	9/2000	Upadhyay et al.	375/144
7,039,417	B2	5/2006	Lyle et al.	455/452.2
2002/0155811	A1	10/2002	Prismantas et al.	455/63
2004/0028003	A1	2/2004	Diener et al.	370/319
2006/0153283	A1 *	7/2006	Scharf et al.	375/148
2008/0299932	A1 *	12/2008	Belogolovy et al.	455/296
2009/0124205	A1 *	5/2009	Aboba et al.	455/63.1

FOREIGN PATENT DOCUMENTS

WO	99/39444	8/1999
WO	01/73956	10/2001

OTHER PUBLICATIONS

www.redlinecommunications.com, RedCONNEX AN-80i Advanced Broadband Wireless Infrastructure Solution.

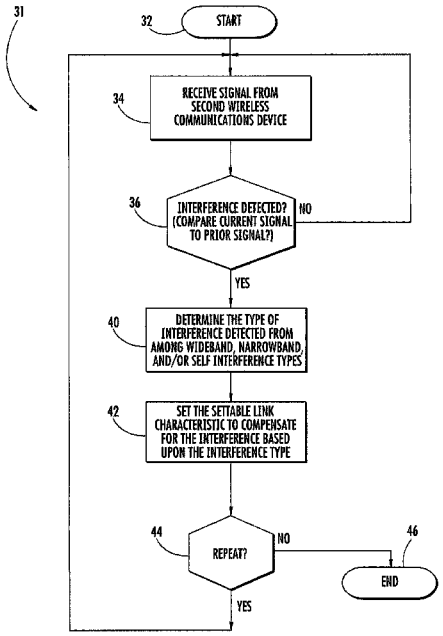
* cited by examiner

Primary Examiner — Zewdu Kassa
(74) *Attorney, Agent, or Firm* — Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A wireless communication system may include first and second wireless communications devices communicating with one another via a wireless communications link having a settable link characteristic. The first and second wireless communications devices may include respective first and second wireless transceivers and respective first and second controllers coupled thereto. The first controller may be for detecting received interference, for determining a type of the interference from among interference types comprising wideband interference and narrowband interference, and for setting the settable link characteristic to compensate for the interference based upon the interference type.

14 Claims, 6 Drawing Sheets



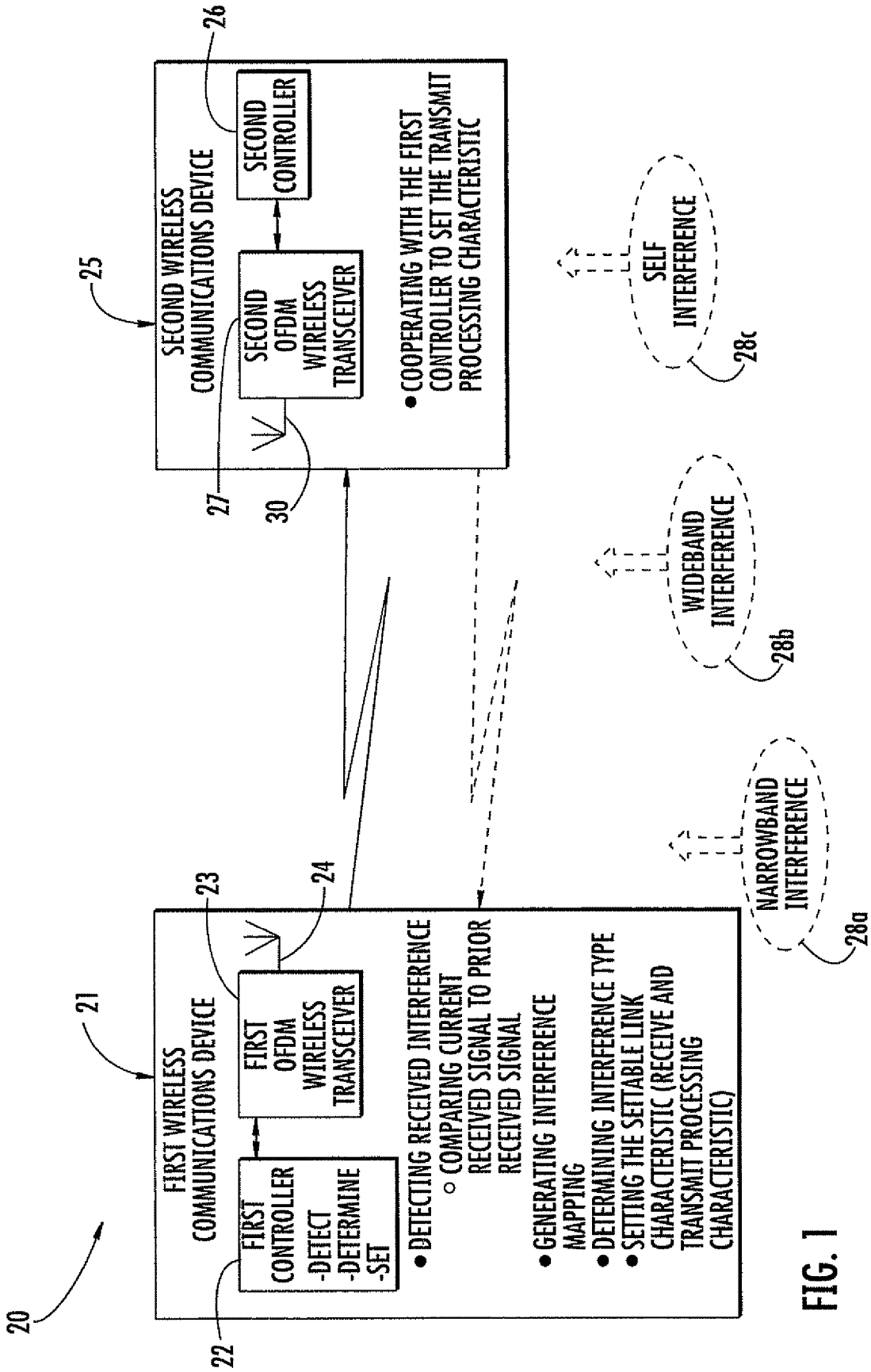

20
21
22
23
24
25
26
27
30
FIRST WIRELESS COMMUNICATIONS DEVICE
FIRST CONTROLLER
-DETECT
-DETERMINE
-SET
FIRST OFDM WIRELESS TRANSCEIVER
SECOND WIRELESS COMMUNICATIONS DEVICE
SECOND CONTROLLER
SECOND OFDM WIRELESS TRANSCEIVER
• DETECTING RECEIVED INTERFERENCE
○ COMPARING CURRENT RECEIVED SIGNAL TO PRIOR RECEIVED SIGNAL
• GENERATING INTERFERENCE MAPPING
• DETERMINING INTERFERENCE TYPE
• SETTING THE SETTABLE LINK CHARACTERISTIC (RECEIVE AND TRANSMIT PROCESSING CHARACTERISTIC)
• COOPERATING WITH THE FIRST CONTROLLER TO SET THE TRANSMIT PROCESSING CHARACTERISTIC
NARROWBAND INTERFERENCE
28a
WIDEBAND INTERFERENCE
28b
SELF INTERFERENCE
28c

FIG. 1

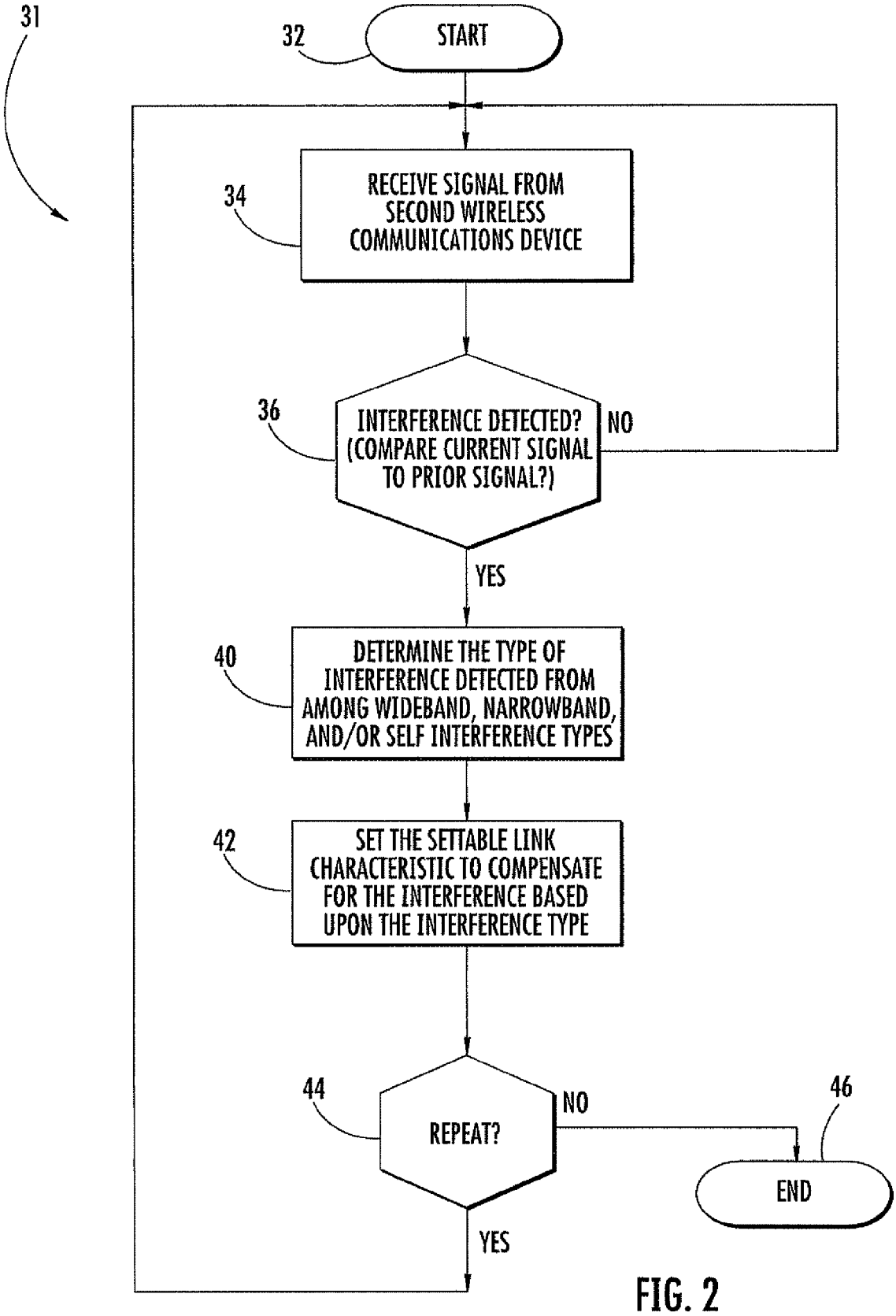

31
32
START
34
RECEIVE SIGNAL FROM SECOND WIRELESS COMMUNICATIONS DEVICE
36
INTERFERENCE DETECTED? (COMPARE CURRENT SIGNAL TO PRIOR SIGNAL?)
NO
YES
40
DETERMINE THE TYPE OF INTERFERENCE DETECTED FROM AMONG WIDEBAND, NARROWBAND, AND/OR SELF INTERFERENCE TYPES
42
SET THE SETTABLE LINK CHARACTERISTIC TO COMPENSATE FOR THE INTERFERENCE BASED UPON THE INTERFERENCE TYPE
44
REPEAT?
NO
46
END
YES

FIG. 2

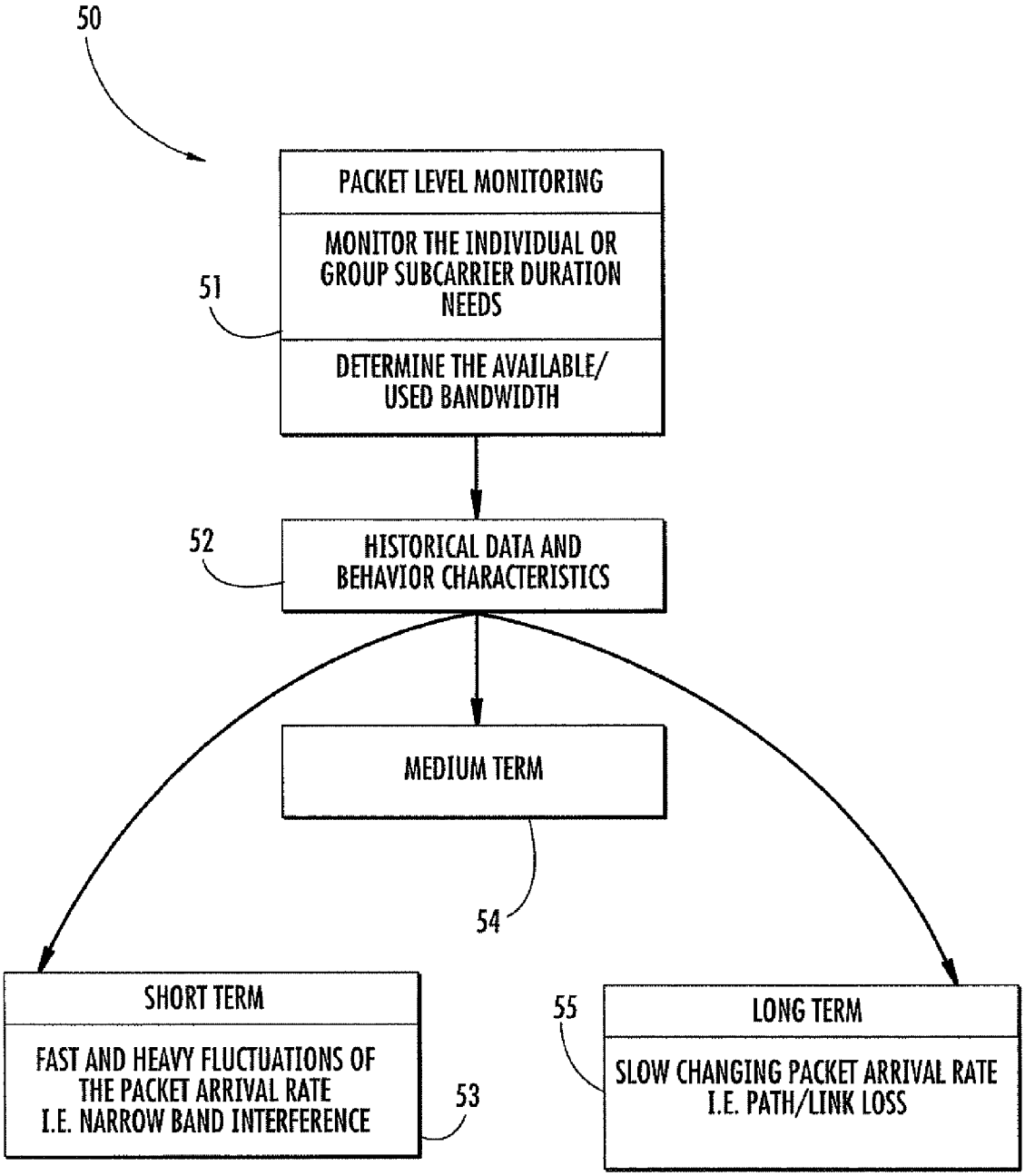

50
PACKET LEVEL MONITORING
MONITOR THE INDIVIDUAL OR GROUP SUBCARRIER DURATION NEEDS
51
DETERMINE THE AVAILABLE/ USED BANDWIDTH
52
HISTORICAL DATA AND BEHAVIOR CHARACTERISTICS
MEDIUM TERM
54
SHORT TERM
FAST AND HEAVY FLUCTUATIONS OF THE PACKET ARRIVAL RATE I.E. NARROW BAND INTERFERENCE
53
55
LONG TERM
SLOW CHANGING PACKET ARRIVAL RATE I.E. PATH/LINK LOSS

FIG. 3

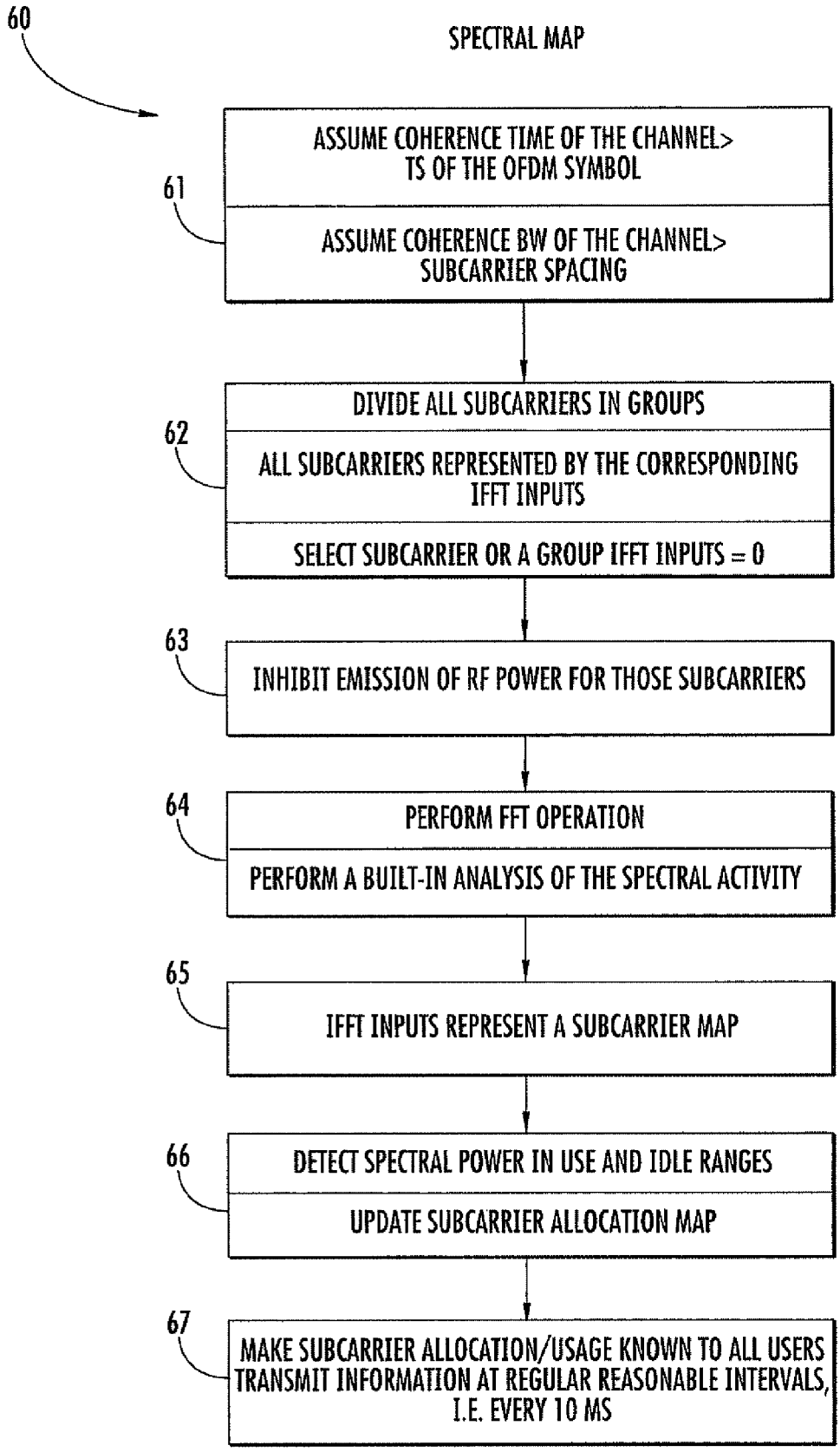

60
SPECTRAL MAP
61
ASSUME COHERENCE TIME OF THE CHANNEL> TS OF THE OFDM SYMBOL
ASSUME COHERENCE BW OF THE CHANNEL> SUBCARRIER SPACING
62
DIVIDE ALL SUBCARRIERS IN GROUPS
ALL SUBCARRIERS REPRESENTED BY THE CORRESPONDING IFFT INPUTS
SELECT SUBCARRIER OR A GROUP IFFT INPUTS = 0
63
INHIBIT EMISSION OF RF POWER FOR THOSE SUBCARRIERS
64
PERFORM FFT OPERATION
PERFORM A BUILT-IN ANALYSIS OF THE SPECTRAL ACTIVITY
65
IFFT INPUTS REPRESENT A SUBCARRIER MAP
66
DETECT SPECTRAL POWER IN USE AND IDLE RANGES
UPDATE SUBCARRIER ALLOCATION MAP
67
MAKE SUBCARRIER ALLOCATION/USAGE KNOWN TO ALL USERS TRANSMIT INFORMATION AT REGULAR REASONABLE INTERVALS, I.E. EVERY 10 MS

FIG. 4

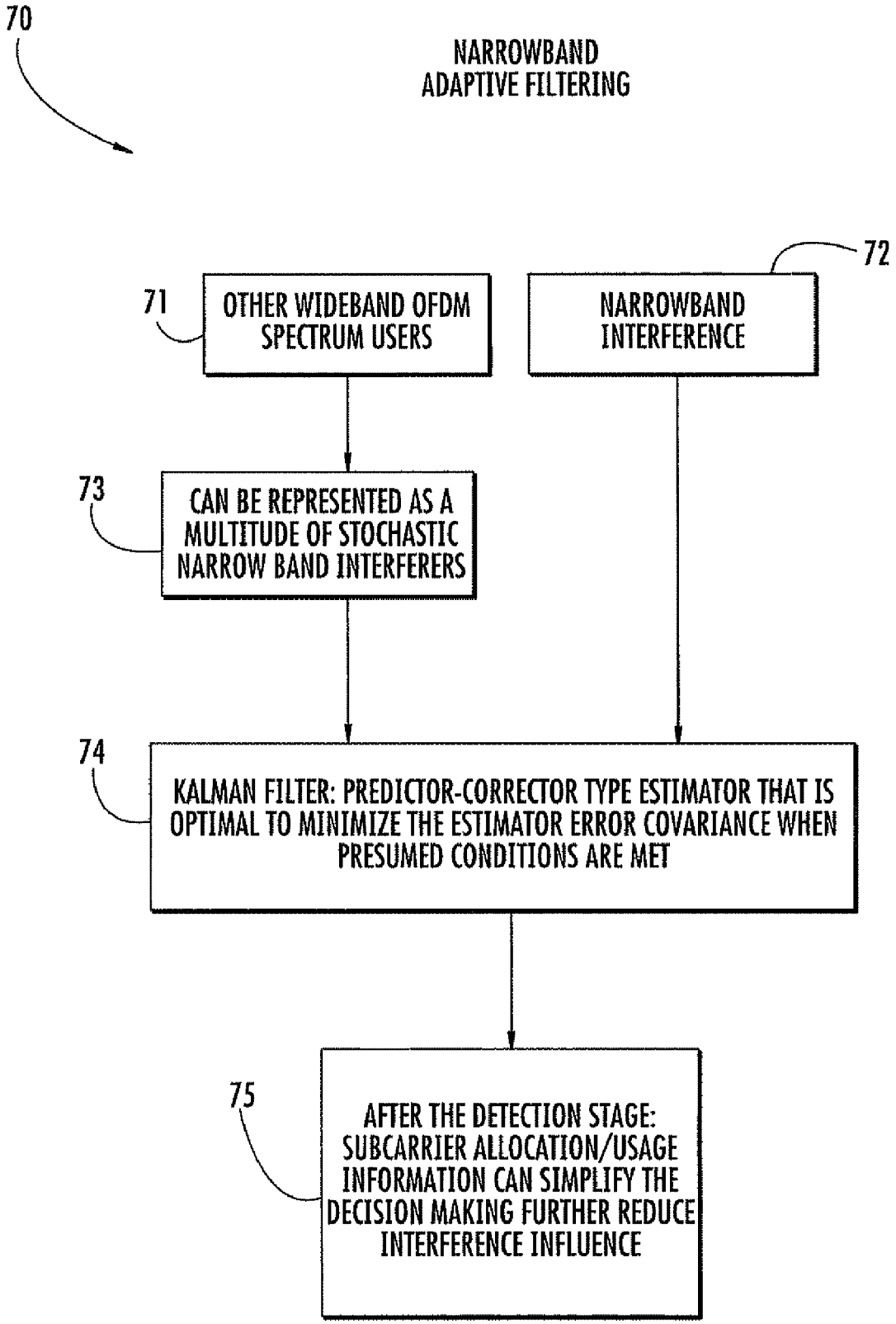

70
NARROWBAND ADAPTIVE FILTERING
71
OTHER WIDEBAND OFDM SPECTRUM USERS
72
NARROWBAND INTERFERENCE
73
CAN BE REPRESENTED AS A MULTITUDE OF STOCHASTIC NARROW BAND INTERFERERS
74
KALMAN FILTER: PREDICTOR-CORRECTOR TYPE ESTIMATOR THAT IS OPTIMAL TO MINIMIZE THE ESTIMATOR ERROR COVARIANCE WHEN PRESUMED CONDITIONS ARE MET
75
AFTER THE DETECTION STAGE: SUBCARRIER ALLOCATION/USAGE INFORMATION CAN SIMPLIFY THE DECISION MAKING FURTHER REDUCE INTERFERENCE INFLUENCE

FIG. 5

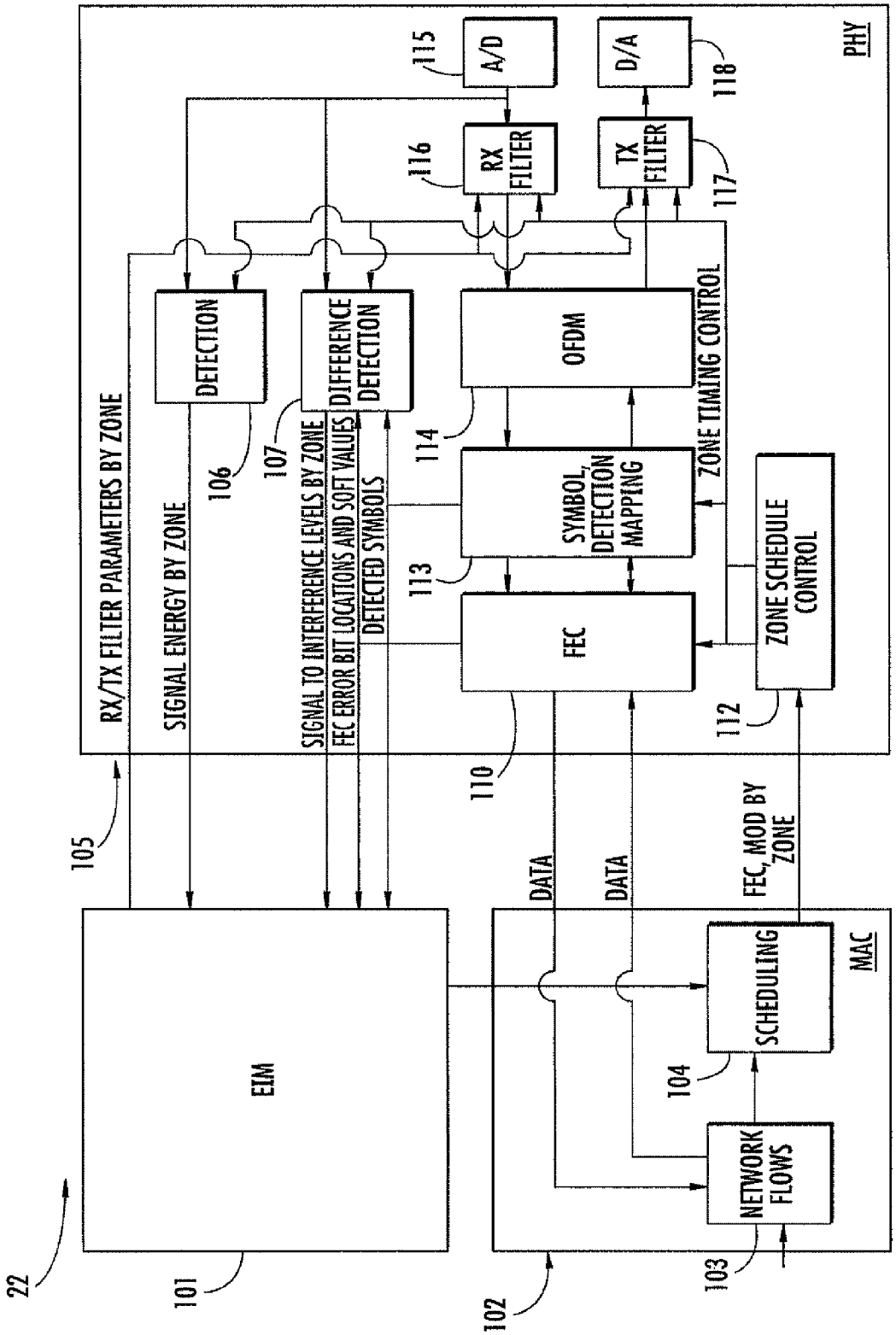

PHY
A/D
D/A
RX FILTER
TX FILTER
DETECTION
DIFFERENCE DETECTION
OFDM
SYMBOL, DETECTION MAPPING
FEC
ZONE SCHEDULE CONTROL
ZONE TIMING CONTROL
RX/TX FILTER PARAMETERS BY ZONE
SIGNAL ENERGY BY ZONE
SIGNAL TO INTERFERENCE LEVELS BY ZONE
FEC ERROR BIT LOCATIONS AND SOFT VALUES
DETECTED SYMBOLS
DATA
DATA
FEC, MOD BY ZONE
EIM
MAC
SCHEDULING
NETWORK FLOWS
22
101
102
103
104
105
106
107
110
112
113
114
115
116
117
118

FIG. 6

WIRELESS COMMUNICATION SYSTEM COMPENSATING FOR INTERFERENCE AND RELATED METHODS

FIELD OF THE INVENTION

The present invention relates to the field of communications, and, more particularly, to interference compensation and related methods.

BACKGROUND OF THE INVENTION

As wireless communications has become prevalent in society, it is not uncommon for two wireless communications devices to interfere with the operation of each other when operating within transmission range of each other. Indeed, this type of interference has become more frequent with increasing wireless connectivity permeating society, such as, cellular phones and mobile email devices. For example, when IEEE 802.11b (WiFi) wireless devices, for example, laptop computers, became readily available to the home consumer, "cordless" home telephones were capable of rendering the WiFi devices inoperable due to interference.

Interference is typically categorized into two types: narrowband interference and wideband interference. Narrowband interference includes forms of interference that are concentrated around a relatively small frequency bandwidth. Several common approaches to compensating for narrowband interference may include, for example, forward error correction (FEC), baseband coding (FHSS/DSSS spread spectrum), diversity in frequency and/or time, and signal cancellation.

Differently, wideband interference includes forms of interference that are spread out across a relatively large frequency bandwidth. Several common approaches to compensating for wideband interference may include, for example, FEC, adaptive data rate (modulation and channel bandwidth), adaptive power control, diversity in frequency and/or timer and signal cancellation.

Another common type of interference is self interference. Common causes of self interference may include, for example, collocation or frequency reuse. In particular, collocation may be caused by two wireless communication systems being deployed too closely together while frequency reuse may be caused by two wireless communication systems using the same frequency band/channel. Several approaches to compensating for self interference, which are available during planning and development stages of wireless communication systems, include, for example, installation (isolation between antennas), frequency planning, antenna pattern manipulation, synchronization of transmitters, and filtering (duplexing).

Although interference is commonly generated inadvertently, another frequent source may be intentionally created by an unauthorized user, e.g. a jammer. Indeed, similar to the cordless home telephone, the unauthorized user may render a wireless communication system inoperable or may reduce the effectiveness, for example, capacity, of the wireless communication system.

Regardless of the source, there is a desire to reduce the effect of interference in communications. For example, high spectral efficiency wireless communications devices, for example, an RF-7800W-OU440, as available from the Harris Corporation of Melbourne, Fla., the assignee of the present application, use high signal-to-noise ratio transmissions and may be susceptible to interference.

An approach to interference in wireless communication systems may be interference compensation. For example, frequency diversity may used to compensate for the interference by adjusting the operating frequency of the wireless communications device to a frequency free of the interference. Another approach to interference compensation is spatial diversity using a plurality of antennas. In this approach, the undesired interference is canceled out using the time shifted variants received at each antenna.

Another approach to interference compensation is disclosed in U.S. Pat. No. 6,115,409 to Upadhyay et al. This system includes an array of antennas for spatial diversity. The system uses the spatial diversity to cancel out the interference. Moreover, the system uses spatial and temporal filters to cancel out wideband and narrowband interference in the antenna array.

Another approach to interference compensation is disclosed in U.S. Pat. No. 7,039,417 to Lyle et al. The system of Lyle et al. cycles through available channels and evaluates the presence of interference on each channel. The system may also determine the type of electronic device causing the interference, i.e. a cell phone or a microwave. The system assigns a quality-of-service parameter for the channel and moves on to the next channel. Using the table of service parameters for each available channel, the system may select a channel that is interference free or subject to low levels of interference. In other words, this system uses frequency diversity to compensate for interference.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide effective interference compensation.

This and other objects, features, and advantages in accordance with the present invention are provided by a wireless communication system comprising first and second wireless communications devices communicating with one another via a wireless communications link having at least one settable link characteristic. The first and second wireless communications devices may include respective first and second orthogonal frequency-division multiplexing (OFDM) wireless transceivers and respective first and second controllers coupled thereto. The first controller may be for detecting received interference, for determining a type of the received interference from among a plurality of interference types comprising wideband interference and narrowband interference, and for setting the at least one settable link characteristic to compensate for the received interference based upon the interference type. Advantageously, the wireless communication system may provide efficient interference compensation based upon the interference type.

The plurality of interference types may further include self interference. Moreover, the first controller may detect the received interference based upon a comparison of a current received signal to at least one prior received signal. The first controller may also repeat the detecting, determining, and setting.

More particularly, the at least one settable link characteristic may comprise at least one receive processing characteristic. The at least one settable link characteristic may comprise at least one transmit processing characteristic. In some embodiments, the first controller may cooperate with the second controller to set the at least one transmit processing characteristic.

Further, the first controller may generate an interference map of the received interference onto OFDM cells. The first

controller may set the at least one settable link characteristic based upon the interference map.

The first controller may determine the interference type based upon at least one of fade characteristics, noise characteristics, and path characteristics. For example, the at least one settable link characteristic may comprise at least one of transmission power, frequency diversity, time diversity, modulation, forward error correction (FEC), channel bandwidth, and adaptive filtering.

Another aspect is directed to a method for compensating interference in a wireless communication system comprising first and second OFDM wireless communications devices communicating with one another via a wireless communications link having at least one settable link characteristic. The method may comprise detecting received interference, determining a type of the interference from among a plurality of interference types comprising wideband interference and narrowband interference, and setting the at least one settable link characteristic to compensate for the interference based upon the interference type.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic diagram of the wireless communication system according to the present invention.

FIG. **2** is a flowchart of a method for compensating interference in the wireless communication system of FIG. **1**.

FIG. **3** is a block diagram for an embodiment of the detection of interference according to the present invention.

FIG. **4** is a block diagram for an embodiment of the generation of an interference map according to the present invention.

FIG. **5** is a block diagram for an embodiment of the narrowband adaptive filtering according to the present invention.

FIG. **6** is a more detailed schematic block diagram of the controller of FIG. **1**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring initially to FIGS. **1-2**, a wireless communication system **20** illustratively includes first **21** and second **25** wireless communications devices. Additionally, the wireless communication system **20** may include more than two wireless communications devices and/or a wireless base station. Alternatively, the wireless communication system **20** may include only one wireless communications device and a wireless base station. The first **21** and second **25** wireless communications devices illustratively communicate with one another via a wireless communications link having a plurality of settable link characteristics. For example, the settable link characteristics include at least one of transmission power, frequency diversity, time diversity, modulation, forward error correction (FEC), channel bandwidth, and adaptive filtering.

The first and second wireless communications devices **21**, **25** illustratively include first and second wireless transceivers **23**, **27**, respective first and second controllers **22**, **26** coupled to the wireless transceivers, and respective first and second antennas **24**, **30** coupled to the wireless transceivers. The first and second wireless transceivers **23**, **27** illustratively comprise respective first and second orthogonal frequency-division multiplexing (OFDM) transceivers.

The method for compensating interference **28***a*-**28***c* in the wireless communication system **20** begins at Block **32**, the first wireless communications device **21** receives a transmission from the second wireless communications device **25** at Block **34**. Illustratively, the transmission from the first wireless communications device **21** to the second wireless communications device **25** is problem free (shown with solid line). Differently, the return transmission is subject to interference **28***a*-**28***c* from an unknown source (shown with dashed line). At decision Block **36**, the first controller **22** illustratively detects whether there is any received interference **28***a*-**28***c*. The first controller **22** may detect the received interference **28***a*-**28***c* based upon a comparison of a current received signal to at least one prior received signal.

More specifically, the first controller **22** may store data associated with past performance of the received signal and compare the current received signal with the stored data to determine whether there is any received interference **28***a*-**28***c*. If no interference **28***a*-**28***c* with the return transmission is detected, the first wireless communications device **21** makes no adjustments and returns to Block **34** to continue to receive the return transmission and transmit any remaining data.

Referring briefly and additionally to FIG. **3**, a diagram **50** shows the first controller **22** detecting the interference **28***a*-**28***c* by at least performing interference parameter estimation. This includes monitoring **51** bit-error rate (BER), signal-to-noise and distortion ratio, and packet retransmission characteristics. These parameters are monitored and compared with history **52** of received signals. The history is broken into short term (seconds) **53**, medium term (hours/days) **54**, and long term (weeks/months) **55** statistics. The comparison of link performance parameters with historical data allows the algorithm to advantageously determine the cause of the degradation in link performance, i.e. is it a short term fade or truly interference.

Referring again to FIGS. **1-2**, if interference **28***a*-**28***c* is detected, the method moves to Block **40** where the first controller **22** determines a type of the interference from among a plurality of interference types comprising narrowband interference **28***a*, wideband interference **28***b*, and self interference **28***c*. The first controller **22** determines the relative bandwidth of the interferer to the operating channel. More specifically, the first controller **22** determines the interference type based upon at least one of fade characteristics (flat or frequency selective), noise characteristics (wideband or narrowband), and path characteristics (line-of-sight or multipath).

For example, measurements made as part of the detection portion of the algorithm may be categorized into regions that map into modulation and FEC parameter selections. For interference-avoidance methods, bandwidth determination may often be adequate. In an interference-avoidance aproach, the interference is detected then communications are conducted in regions or zones free from or with minimal interference.

Interference coexistence approaches subdivide in two categories: transmit parameters, such as, modulation type for FEC parameters; and reception processing, such as, adaptive filtering, demodulation decision-region adjustment, or turbo-code transition-probability adjustment.

For interference coexistence methods, the detection schemes may be augmented to become estimation processes to allow for more effective optimization. More parameters

may be measured; consequently, this may lead to other categorizations. Also, a monitoring process may be implemented with the algorithm method to adaptively adjust these regions based on effectiveness, based upon a closed-loop process to ensure convergence and stability. Advantageously, probability of success (or equivalently minimized BER) is increased.

Several techniques may be used to accomplish this. The first technique may include scanning a sample of the available channels. The receiver scans the designated operating channels and records the noise floor on each one. A map is created to determine the extent of the interfering source. In the event that the interference appears to be isolated to a small portion of the band, further scans using a smaller step size may be initiated to refine the breadth of the interfering source.

The second technique involves changing the operating channel bandwidth. This may apply to links that are using the 20 MHz or 40 MHz bandwidth setting. The categorization algorithm may monitor the noise floor on the channel at the wider and narrower bandwidths. If the bandwidth is reduced by one half but the noise floor remains constant, then the interferer is narrower than the channel bandwidth. If the noise floor is reduced by one half, then the interferer is wider than the channel bandwidth.

The third technique uses signal processing centered on the Fourier transform associated with the OFDM. The bandwidth of the interferer can be determined through analysis of the spectral components, shown in a diagram **60** of FIG. **4**. The method for spectral mapping beings by making assumptions about the coherence time of the channel **61**. The OFDM map is then subdivided **62** into groups. Subsequently, a selected group of subcarriers has their emission suspended **63**. The fast Fourier transform (FFT/IFFT) is then performed **64** to provide a subcarrier map **65**. The spectral power in use and idle ranges are calculated **66**. Lastly, subcarrier allocation/usage is transmitted **67** to all users.

Referring again to FIGS. **1-2**, at Block **42**, the first controller **22** sets the settable link characteristics to compensate for the interference based upon the interference type. The settable link characteristics may comprise at least one receive processing characteristic and/or at least one transmit processing characteristic. The first controller **22** illustratively cooperates with the second controller **26** to set the at least one transmit processing characteristic. In some embodiments, the first controller **22** may independently set the transmit processing characteristic.

The first controller **22** may selectively set the settable link characteristics. In other words, the first controller **22** applies a "recipe" of interference compensation to communications, the recipe being based upon the type of interference detected and a pre-existing priority based algorithm. The following lists give the priority of application for settable link characteristics for narrowband and wideband interferers.

Narrowband Compensation
1. Adaptive power control
2. Narrowband adaptive filtering
3. Adaptive waveform
4. Adaptive channel bandwidth
5. Diversity in Frequency—change operating frequency

Wideband Compensation:
1. Adaptive power control
2. Adaptive guard band—use Spectral Map, subcarrier allocation information to deactivate subcarrier
3. Narrowband adaptive filtering
4. Adaptive waveform
5. Adaptive channel bandwidth
6. Diversity in Frequency—change operating frequency
7. Diversity in Time
   a. Change OFDM symbol time
   b. Change OFDM symbol duration for cyclic extension

Flexibility to distribute the algorithms, providing enhanced monitoring and more direct compensation to the signal itself, may give better results.

Adaptive power control may permit the first and second wireless communications devices **21**, **25** to negotiate transmit power based upon transmission characteristics. By enabling the increase of transmit power to overcome interference sources, it is possible to burn through the interference and therefore increase the signal-to-noise/interference ratio. This method of compensation may be simple and efficient, and should be used as a first line of defense, being noted as the first priority in both compensation method lists above. It is also applicable to narrow and wideband interference **28***a*-**28***b* sources but not for collocation issues.

Frequency diversity techniques compensate for the interference by changing the operating frequency. This includes techniques, such as, intelligent channel selection where a radio scans its available spectrum and moves to a clean frequency. This technique can be effective at maintaining the data throughput but can require frequency coordination between the first and second wireless communications devices **21**, **25**.

Diversity in time can be an effective technique for packet based systems that are receiving interference from a pulsed source. By modifying the frame timing, it may be possible to align the pulsed interference to be out of sequence with the desired transmission between the first and second wireless communications devices **21**, **25**. This may be effective in point-to-multipoint mode where a master can choose the point in time that it uses to transmit to any particular slave (avoiding local interference at the slave).

Adaptive waveform (modulation and FEC) may be adapted based on the amount and type of interference **28***a*-**28***c*. This includes changing the modulation type and/or the FEC rate to change the required signal-to-noise ratio of the system. The appropriate waveform for any specific type of interference **28***a*-**28***c* is dependent on the amount and type of interference that is present. It may be helpful to recognize the type of interference **28***a*-**28***c* when using an adaptive waveform technique. There can be significant differences in system performance that result from matching the correct waveform with the interference **28***a*-**28***c*. For instance, the process gain that results from different error correction techniques is dependent on the cause of the errors (Reed-Solomon works better for burst errors and convolutional coding works better for random errors). Therefore, it may be helpful to tailor the adaptive waveform algorithm to the type of interference **28***a*-**28***c*.

In addition to changing the waveform (described above), the channel bandwidth can also be changed to compensate for interference **28***a*-**28***c*. If the interfering source is wideband, the interferer will appear to be more like Gaussian noise and narrowing the channel bandwidth will reduce the noise within the channel. This improves the overall signal-to-noise ratio by sacrificing channel throughput. However, the opposite may be true for narrowband interferers. If the bandwidth of the interferer is narrower than the channel bandwidth, narrowing the channel bandwidth will result in a higher level of interference **28***a*-**28***c* within the receiver. Therefore, it may be helpful that the interference **28***a*-**28***c* be characterized before an interference compensation technique is chosen.

Spatial diversity for signal cancellation or the use of multiple antennas (MIMO) may create an opportunity to use active cancellation to compensate for interference **28***a*-**28***c*.

The theory behind MIMO is that the multiple antennas receive time shifted versions of a desired and undesired signal. Signal processing is then used to shift the desired signal into phase alignment and the undesired signal out of phase alignment (180 degrees out of phase). This shift in the phase of the signal may result in an improvement in desired signal power and a significant reduction in undesired signal power, therefore improving the overall signal-to-interference ratio. The use of spatial diversity for signal cancellation may not affect the data throughput of the channel and this method should be considered to be one of the primary interference mitigation methods for both wideband **28***b* and narrowband interference **28***a*.

Null steering can also be used as an interference mitigation technique. This method uses the capability of detecting the direction of arrival for the received interference **28***a*-**28***c*. Once the azimuth is determined, a null in the antenna pattern can be steered in the direction of the interfering source. This method works for both wideband and narrowband interferers and adaptive and fixed antenna patterns. However, it does uses either a mechanical or electronically steered antenna. Advantageously, significant reductions in interference power can be achieved using this method.

Referring again to FIGS. **1**-**2**, at decision Block **44**, the first controller **22** may optionally repeat the detecting, determining, and setting by returning to Block **34**. In other words, the first controller **22** may apply its interference compensation algorithm iteratively. If the received signal does not return to a historical state indicative of interference free transmission, the method returns to Block **34** and the setting of settable link characteristics at Block **42** is adjusted appropriately, i.e. feedback analysis. If the received signal returns to normal historical performance, the method ends at Block **46**.

In the embodiments where the first and second wireless communications devices **21**, **25** include OFDM transceivers, the first controller **22** generates an interference map of the received interference **28***a*-**28***c* onto OFDM cells. Moreover, the first controller **22** sets the settable link characteristics based upon the interference map.

Referring to FIG. **5**, a detailed and exemplary illustration of the algorithm for interference compensation is illustrated. Narrowband adaptive filtering (diagram **70**) includes dividing the dividing the interference into wideband (from other wideband OFDM spectrum users) **71** and narrowband **72**. The wideband interference is represented **73** as a plurality of stochastic narrowband interferers. A Kalman filter is then applied **74**. The subcarrier allocation/usage information is then used **75** in the decision making process.

Referring specifically to FIGS. **1** and **6**, the first controller **22** illustratively includes an enhanced interference mitigation (EIM) module **101**, a media access control (MAC) module **102** coupled to the EIM module, and a physical layer (PHY) module **105** coupled to the EIM module and MAC module. The MAC module **102** includes a network flows block **103** and scheduling block **104** coupled to each other.

The EIM module **101** may execute the EIM algorithms and uses available detection data to build a map of the OFDM cells. This map is provided as input to the scheduling block **104** for informing what FEC and modulation can be used for each zone. As will be appreciated by those skilled in the art, the zone sizes and shapes may be implementation-dependent. Zone types that could span the space from a fixed zone with single symbol duration across subcarriers to a more flexible zone assignment scheme where each symbol duration/subchannel could be assigned a maximum permissible FEC/modulation setting.

The EIM module **101** may request the scheduling block **104** to schedule zones free of transmissions to be used for measurements. The EIM module **101** can vary in sophistication from simply detecting interference levels and recommending frequency switches to highly complex Kalman or H-infinity tracking algorithms, for example.

The network flows block **103** is the source and sink for data referred to as "service flows" or that use the MAC module **102**. Quality-of-Service (QoS) and other factors may establish the priority of each flow. The network flows block **103** uses available information from the PHY module **105** based algorithms to determine a good performance metric for a given interference environment. This metric may comprise, for example, a priority-weighted aggregate flow rate through a node.

The scheduling block **104** uses the data from the EIM module **101** along with the network flows requested data rates and associated priorities to schedule data transmission and reception. The data is placed into zones using the EIM maps to optimize the aggregate priority-weighted flow rate. Further, special modes, such as, mesh and coordinating with other nodes in own network, can be performed here, requiring a level of distributed scheduling.

The PHY module **105** includes a detection block **106** for determining if interference **28***a*-**28***c* exists in the received signal and measuring the amount of energy in a specified OFDM cell. The detection block **106** is for zones that have been designated to be free of transmission so that all the detected energy is from interfering sources. This type of block can also make use of cells that include pilot tones to make signal-to-interference measurements since the signal structure of the pilot is known. The detection block **106** processing can vary in complexity from simple power measurement to more complex signal-processing code—for the pilot carrier cells and for characterizing the signal for cases where knowledge of signal structure will help with more effective compensation.

The PHY module **105** illustratively includes a difference detection block **107** for performing signal-to-interference measurements. The difference detection block **107** includes stored algorithms that can use detected signal and FEC data to reconstruct the signal of interest and effectively subtract it from the raw signal to generate signal-to-interference estimates for any specified cell.

The PHY module **105** illustratively includes a FEC block **110** for performing the error correction encoding and decoding. Overall, the FEC block **110** contributes to EIM by including a large number of algorithms and settings to allow finer compensation granularity. The FEC block **110** interfaces with the difference detection block **107** by including a wider range of algorithms to increases the observability compared to the difference detection block described above. For example, if the algorithms determine exact errors bits and soft error values or certainties, then that can be used to better characterize the interference **28***a*-**28***c*.

The PHY module **105** illustratively includes a symbol detection and mapping (SDM) block **113** that is similar to the FEC block **110** except modulations and detection algorithms are used in place of error-correcting code. The PHY module **105** also illustratively includes an OFDM block **114** for interfacing with the EIM module **101** by providing the number of frequency bandwidths, carrier spacing, and FFT sizes it supports.

The PHY module **105** illustratively includes an Rx filter block **116** for filtering the signal and compensating for the effects of the interference **28***a*-**28***c*. This block may be programmed for zone and anticipated reception. The PHY mod-

ule **105** illustratively includes a Tx filter block **117** for filtering that compensates for the effects of the interference **28***a*-**28***c* by applying an inverse matched filter, for example. The Tx filter block **117** may be programmed for zone and anticipated reception.

The PHY module **105** illustratively includes a Zone Schedule Control (ZSC) block **112** for providing an increase in the ability to compensate based on increased flexibility that can be used to place service flow data in zones. The PHY module **105** illustratively includes a analog-to-digital converter **115** feeding into the Rx filter block **116**, and a digital-to-analog converter **118** receiving the output of the Tx filter block **117**.

This exemplary algorithm may be applied to narrowband and wideband interference **28***a*-**28***b*. The wireless communication system **20** may associate narrowband interference with the following characteristics: OFDM synchronization and frame detection are intermittent. The subcarrier interference may be associated with a single subcarrier or with groups thereof. The known data symbols in the preamble and pilots are continuously correlated with stored/delayed versions of each other.

The wireless communication system **20** may then filter narrowband interference **28***a* adaptively by at least combining subcarrier allocation/usage information with narrowband filtering carried out in existing FFT/IFFT processing. The interference **28***a*-**28***c* may be suppressed before the preamble is fed into the correlation module. When the frequency offset is less than 1% of subcarrier spacing, then it is accurate enough to maintain orthogonality of the OFDM signals.

Wideband interference **28***b* may be detected when interference is caused by WiFi wireless devices or other wideband systems operating in the operating spectrum of the wireless communication system **20**. The side lobes of the sinc-shaped spectra on each subcarrier interfere with subcarriers in use by other systems. The subcarriers in use by the other systems may not be orthogonal with the wireless communication system **20**. Power control information may be used, for example, mean interference power difference being large (several percentage points) between subcarriers with and without interference **28***a*-**28***c*. An adaptive guard band may also be used by deactivating one or more subcarriers adjacent to the subcarriers experiencing the interference **28***a*-**28***c*. For longer OFDM duration, time domain windowing for OFDM symbols may be used—root raised cosine windows sharpen the spectral pulses on each subcarrier and lower the side lobes resulting in less interference power.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A wireless communication system comprising:

first and second wireless communications devices configured to communicate with one another via a wireless communications link having at least one settable link characteristic;

said first and second wireless communications devices comprising respective first and second orthogonal frequency-division multiplexing (OFDM) wireless transceivers and respective first and second controllers coupled thereto and configured to store short term and long term historical characteristics of interference;

said first controller configured to

detect received interference,

determine a type of the received interference from among a plurality of interference types comprising wideband interference, self interference, and narrowband interference based upon comparing at least one characteristic of a current received signal with the short term and long term historical characteristics of interference, and

set the at least one settable link characteristic to compensate for the received interference based upon the interference type.

2. The wireless communication system according to claim **1** wherein said first controller is configured to repeat the detecting, determining, and setting.

3. The wireless communication system according to claim **1** wherein the at least one settable link characteristic comprises at least one receive processing characteristic.

4. The wireless communication system according to claim **1** wherein the at least one settable link characteristic comprises at least one transmit processing characteristic; and wherein said first controller is configured to cooperate with said second controller to set the at least one transmit processing characteristic.

5. The wireless communication system according to claim **1** wherein said first controller is configured to generate an interference map of the received interference onto OFDM cells.

6. The wireless communication system according to claim **5** wherein said first controller is configured to set the at least one settable link characteristic based upon the interference map.

7. The wireless communication system according to claim **1** wherein said first controller is configured to determine the interference type based upon at least one of fade characteristics, noise characteristics, and path characteristics.

8. The wireless communication system according to claim **1** wherein the at least one settable link characteristic comprises at least one of transmission power, frequency diversity, time diversity, modulation, forward error correction (FEC), channel bandwidth, and adaptive filtering.

9. A wireless communications device operable to communicate with an other wireless communications device via a wireless communications link having at least one settable link characteristic, the wireless communications device comprising:

an orthogonal frequency-division multiplexing (OFDM) wireless transceiver; and

a controller coupled to said wireless transceiver and configured to store short term and long term historical characteristics of interference;

said controller configured to

detect received interference,

determine a type of the received interference from among a plurality of interference types comprising wideband interference, self interference, and narrowband interference based upon comparing at least one characteristic of a current received signal with the short term and long term historical characteristics of interference, and

set the at least one settable link characteristic to compensate for the received interference based upon the interference type.

10. The wireless communications device according to claim **9** wherein the at least one settable link characteristic comprises at least one receive processing characteristic.

11. The wireless communications device according to claim **9** wherein the at least one settable link characteristic

comprises at least one transmit processing characteristic; and wherein said controller is configured to cooperate with the other wireless communications device to set the at least one transmit processing characteristic.

12. A method for compensating interference in a wireless communication system comprising first and second orthogonal frequency-division multiplexing (OFDM) wireless communications devices communicating with one another via a wireless communications link having at least one settable link characteristic, the method comprising:

detecting received interference;

storing short term and long term historical characteristics of interference;

determining a type of the received interference from among a plurality of interference types comprising wideband interference, self interference, and narrowband interference based upon comparing at least one characteristic of a current received signal with the short term and long term historical characteristics of interference; and

setting the at least one settable link characteristic to compensate for the received interference based upon the interference type.

13. The method according to claim **12** further comprising repeating the detecting, determining, and setting.

14. The method according to claim **12** wherein the at least one settable link characteristic comprises at least one transmit processing characteristic; and

further comprising cooperating between the first and second wireless communications devices to set the at least one transmit processing characteristic.

* * * * *

Exhibit 2

US007110779B2

(12) **United States Patent**
Billhartz et al.

(10) **Patent No.: US 7,110,779 B2**
(45) **Date of Patent: Sep. 19, 2006**

(54) **WIRELESS COMMUNICATIONS SYSTEM INCLUDING A WIRELESS DEVICE LOCATOR AND RELATED METHODS**

(75) Inventors: **Thomas Jay Billhartz**, Melbourne, FL (US); **Vivek Krishna**, Palm Bay, FL (US); **Steve Kopman**, Melbourne, FL (US)

(73) Assignee: **Harris Corporation**, Mebourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 295 days.

(21) Appl. No.: **10/767,794**

(22) Filed: **Jan. 29, 2004**

(65) **Prior Publication Data**

US 2005/0170843 A1 Aug. 4, 2005

(51) **Int. Cl.**
H04B 1/04 (2006.01)

(52) **U.S. Cl.** **455/456.2**; 455/456.1; 455/456.5; 455/456.6; 342/457; 370/328

(58) **Field of Classification Search** 455/422.1, 455/41.2, 456.1–457, 67.13, 63.4, 67.16, 455/550.1, 562.1, 575.7; 370/328, 352; 342/457–458

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,526,357	A	6/1996	Jandrell	370/95.2
5,550,549	A	8/1996	Procter, Jr. et al.	342/47
5,687,196	A	11/1997	Proctor, Jr. et al.	375/347
5,706,010	A	1/1998	Franke	342/47
6,292,665	B1	9/2001	Hildebrand et al.	455/456
6,680,923	B1 *	1/2004	Leon	370/328
6,865,394	B1 *	3/2005	Ogino et al.	455/456.1
2002/0080759	A1	6/2002	Harrington et al.	370/338
2002/0118655	A1	8/2002	Harrington et al.	370/328
2002/0171586	A1 *	11/2002	Martorana et al.	342/458
2003/0025602	A1	2/2003	Medema et al.	340/568.1
2003/0034887	A1	2/2003	Crabtree et al.	340/539
2003/0043073	A1	3/2003	Gray et al.	342/465
2003/0162550	A1 *	8/2003	Kuwahara et al.	455/456
2003/0182052	A1 *	9/2003	DeLorme et al.	701/201
2003/0191604	A1 *	10/2003	Kuwahara et al.	702/150
2004/0081139	A1 *	4/2004	Beckmann et al.	370/352
2004/0110514	A1 *	6/2004	Kim et al.	455/456.1
2004/0203889	A1 *	10/2004	Karaoguz	455/456.1
2004/0266348	A1 *	12/2004	Deshpande et al.	455/41.2

(Continued)

OTHER PUBLICATIONS

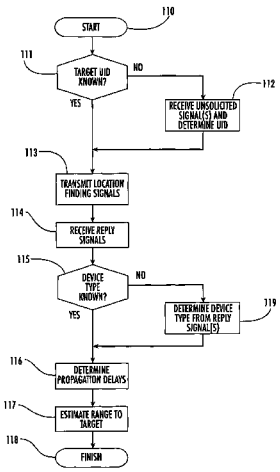
Yellowjacket-A, 802.11a Wi-Fi Analysis System, Berkeley Varitronics Systems.

Primary Examiner—Joseph Feild
Assistant Examiner—Kamran Afshar
(74) *Attorney, Agent, or Firm*—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A wireless communications system may include a plurality of wireless communications devices and a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality thereof. The target device may transmit a respective reply signal for each of the location finding signals. Additionally, the controller may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target device. As such, the controller may estimate a range to the target device based upon a plurality of determined propagation delays.

34 Claims, 9 Drawing Sheets



U.S. PATENT DOCUMENTS

2005/0037775 A1* 2/2005 Moeglein et al. 455/456.1

2005/0059411 A1* 3/2005 Zhengdi 455/456.1

* cited by examiner

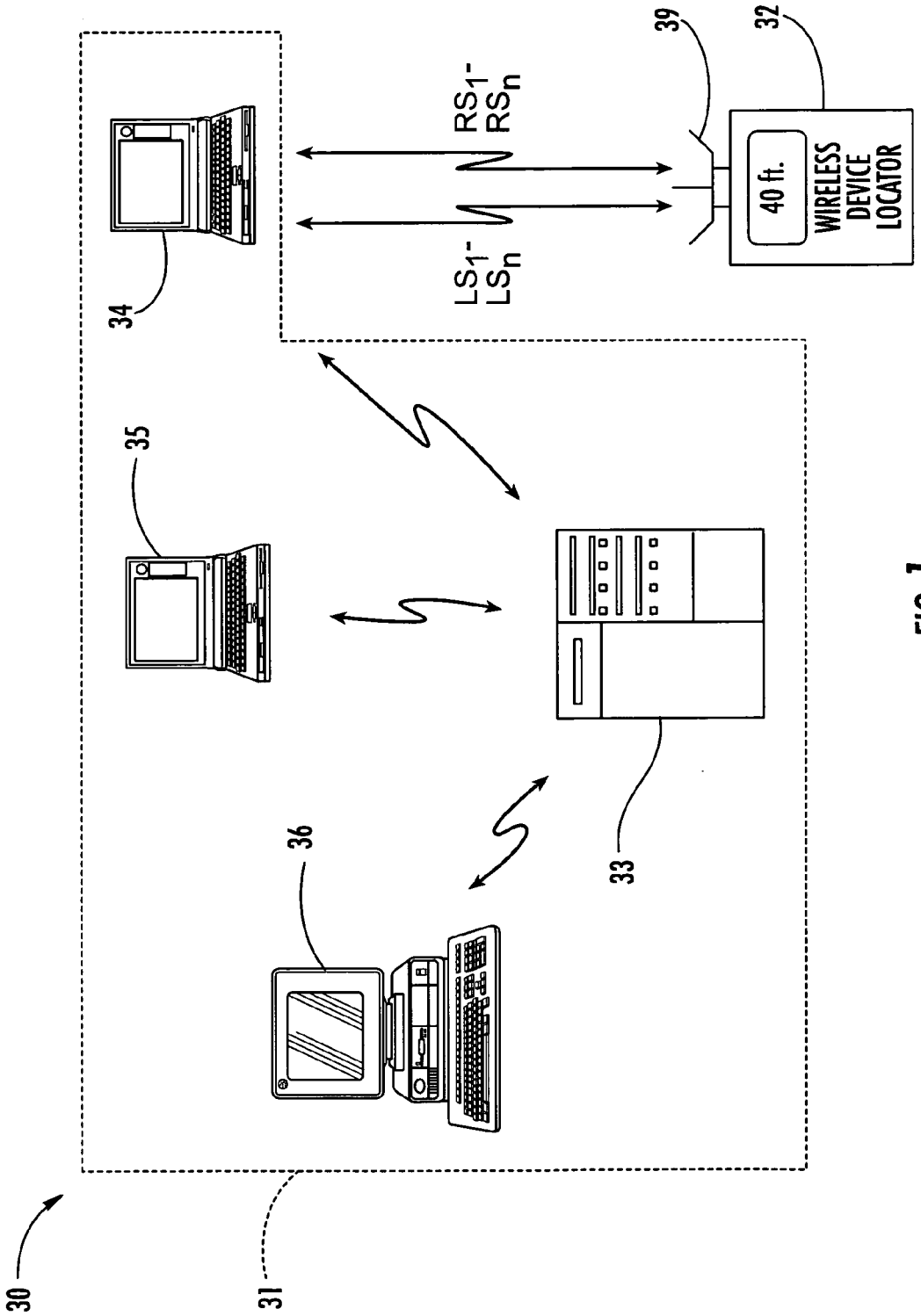

30
31
34
35
36
33
39
32
RS1-
RSn
LS1-
LSn
40 ft.
WIRELESS
DEVICE
LOCATOR

FIG. 1

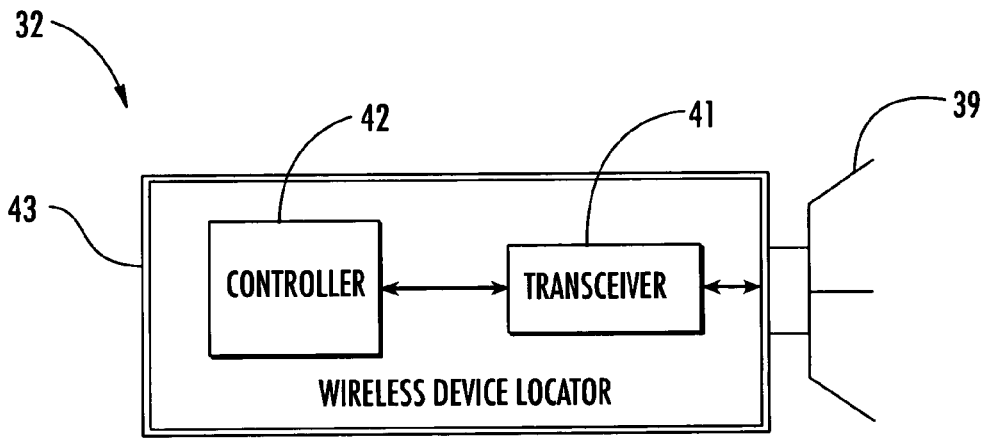

32
42
41
39
43
CONTROLLER
TRANSCEIVER
WIRELESS DEVICE LOCATOR

FIG. 2

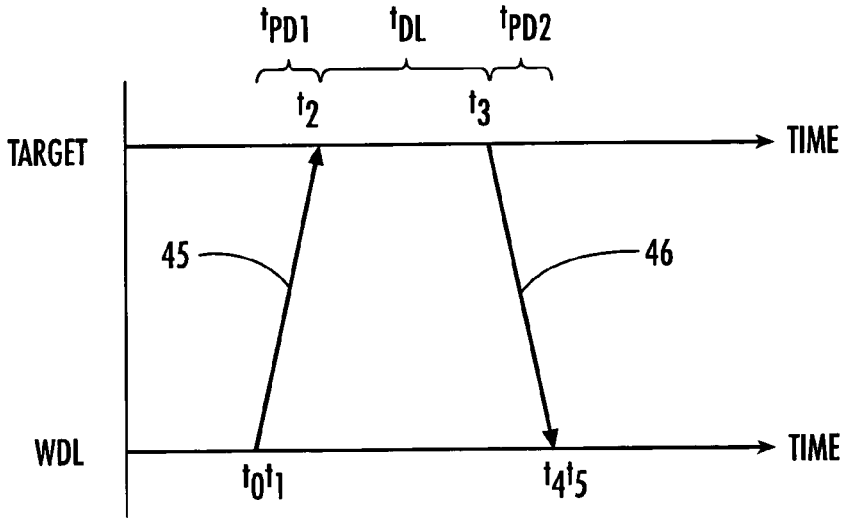

tPD1
tDL
tPD2
t2
t3
TARGET
TIME
45
46
WDL
TIME
t0t1
t4t5

FIG. 3

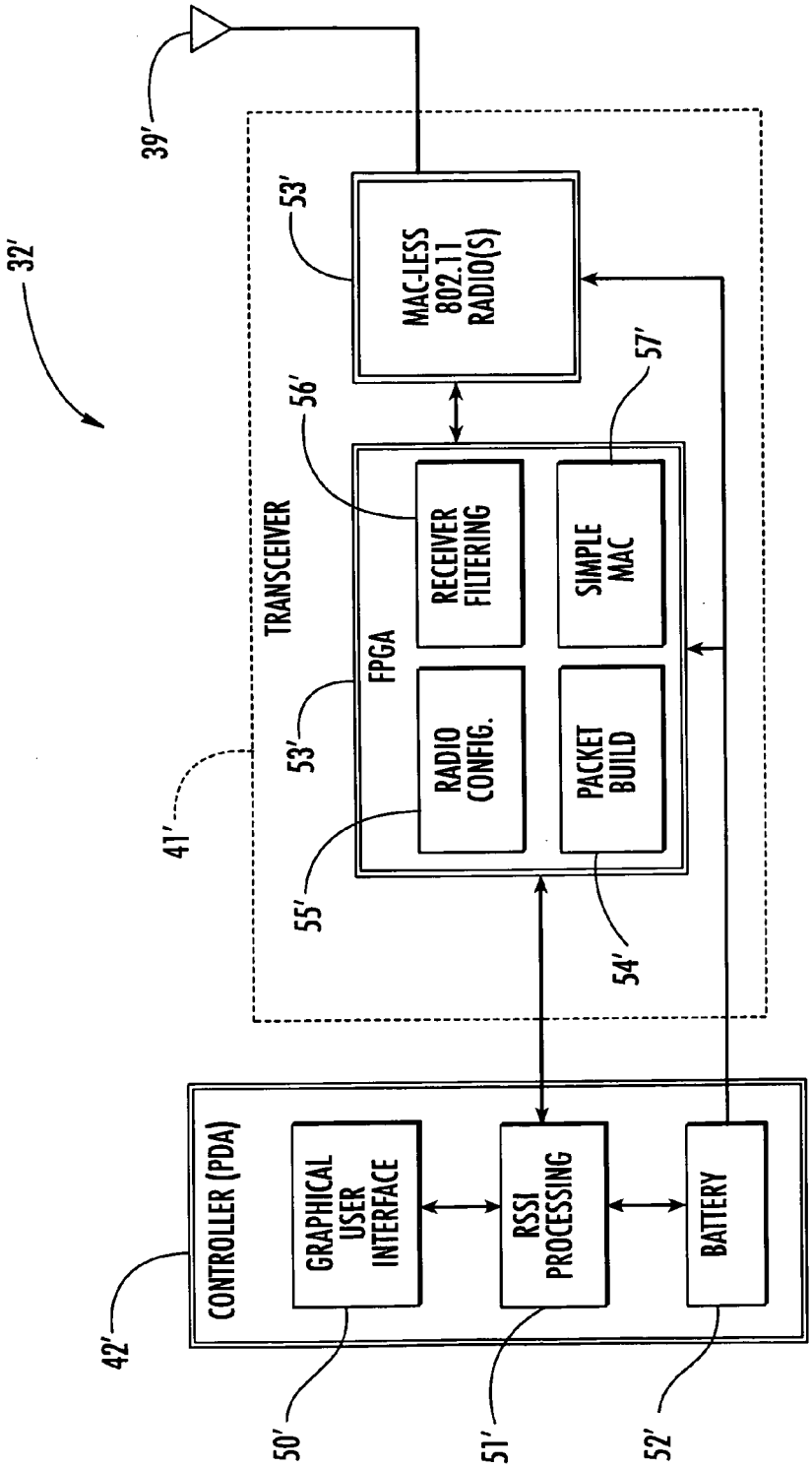

32'
39'
53'
MAC-LESS 802.11 RADIO(S)
56'
57'
TRANSCEIVER
FPGA
RECEIVER FILTERING
SIMPLE MAC
53'
RADIO CONFIG.
PACKET BUILD
41'
55'
54'
CONTROLLER (PDA)
GRAPHICAL USER INTERFACE
RSSI PROCESSING
BATTERY
42'
50'
51'
52'

FIG. 4

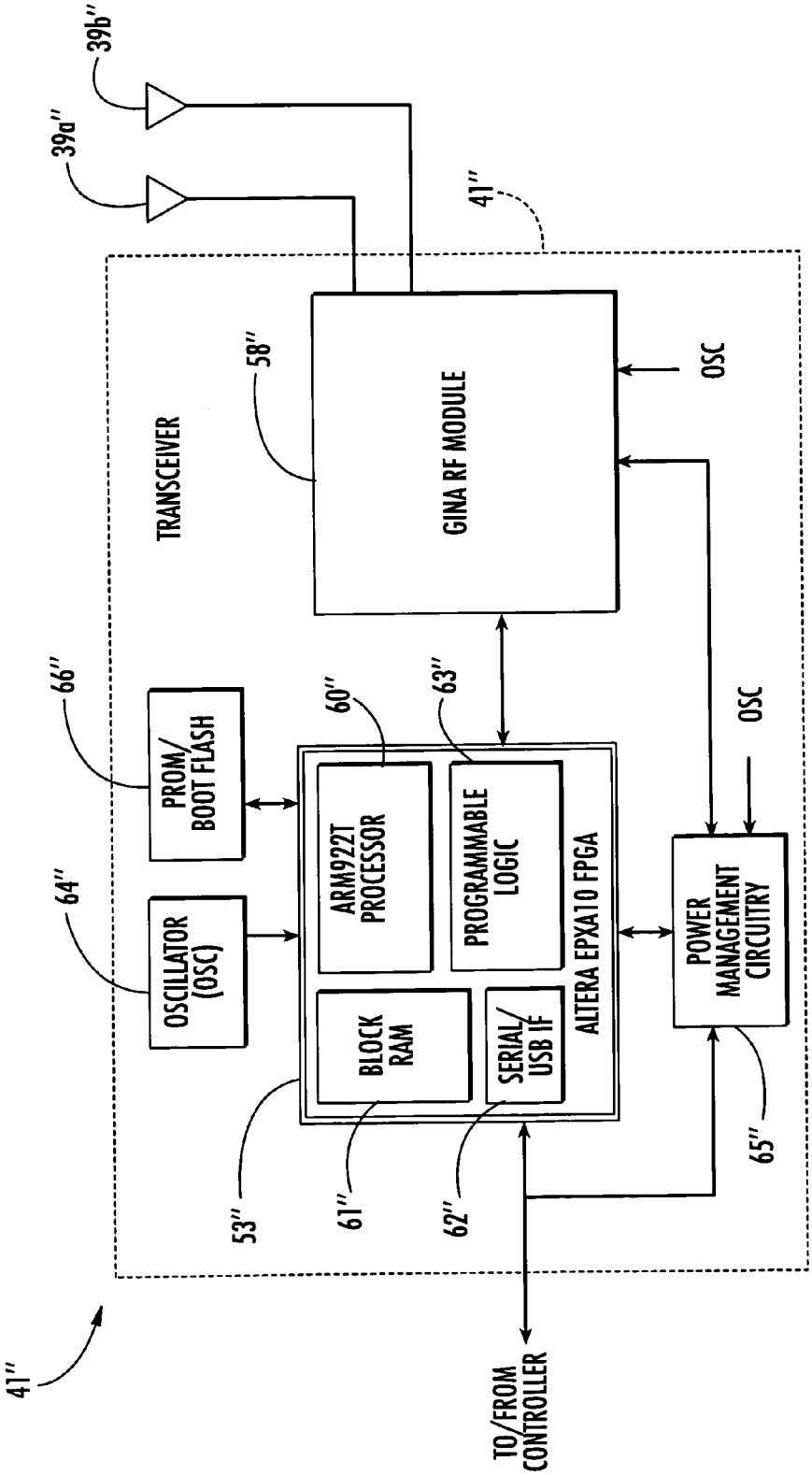

39b''
39a''
41''
TRANSCEIVER
58''
GINA RF MODULE
OSC
66''
PROM/ BOOT FLASH
60''
63''
ARM922T PROCESSOR
PROGRAMMABLE LOGIC
ALTERA EPXA10 FPGA
OSC
64''
OSCILLATOR (OSC)
BLOCK RAM
SERIAL/ USB IF
POWER MANAGEMENT CIRCUITRY
53''
61''
62''
65''
41''
TO/FROM CONTROLLER

FIG. 5

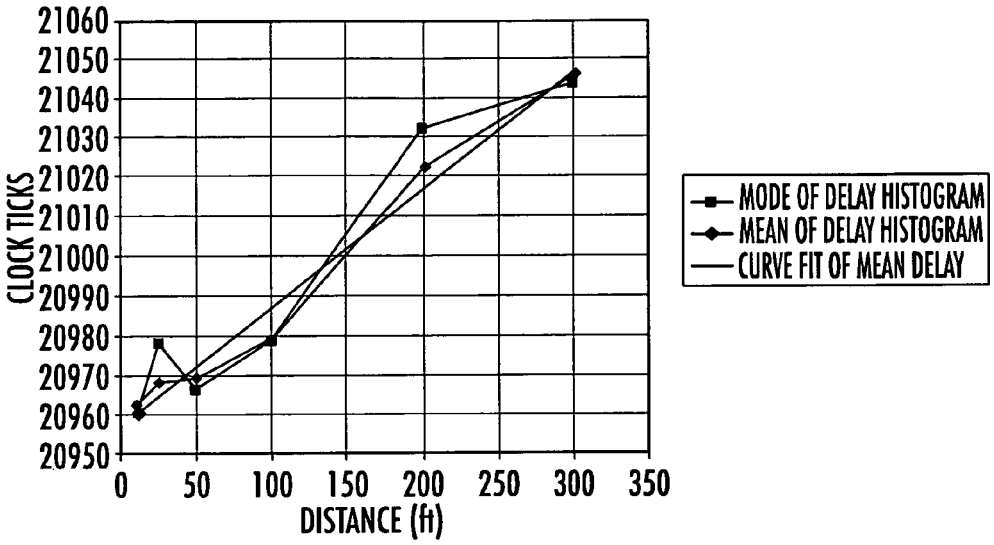

21060
21050
21040
21030
21020
21010
21000
20990
20980
20970
20960
20950
CLOCK TICKS
0
50
100
150
200
250
300
350
DISTANCE (ft)
MODE OF DELAY HISTOGRAM
MEAN OF DELAY HISTOGRAM
CURVE FIT OF MEAN DELAY

FIG. 6

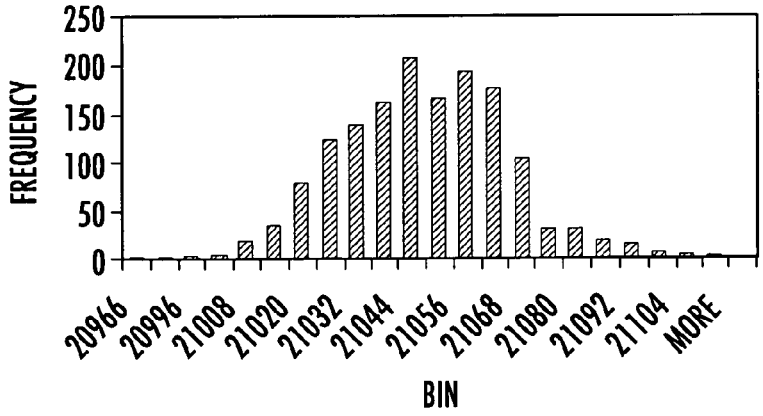

250
200
150
100
50
0
FREQUENCY
20966
20996
21008
21020
21032
21044
21056
21068
21080
21092
21104
MORE
BIN

FIG. 7

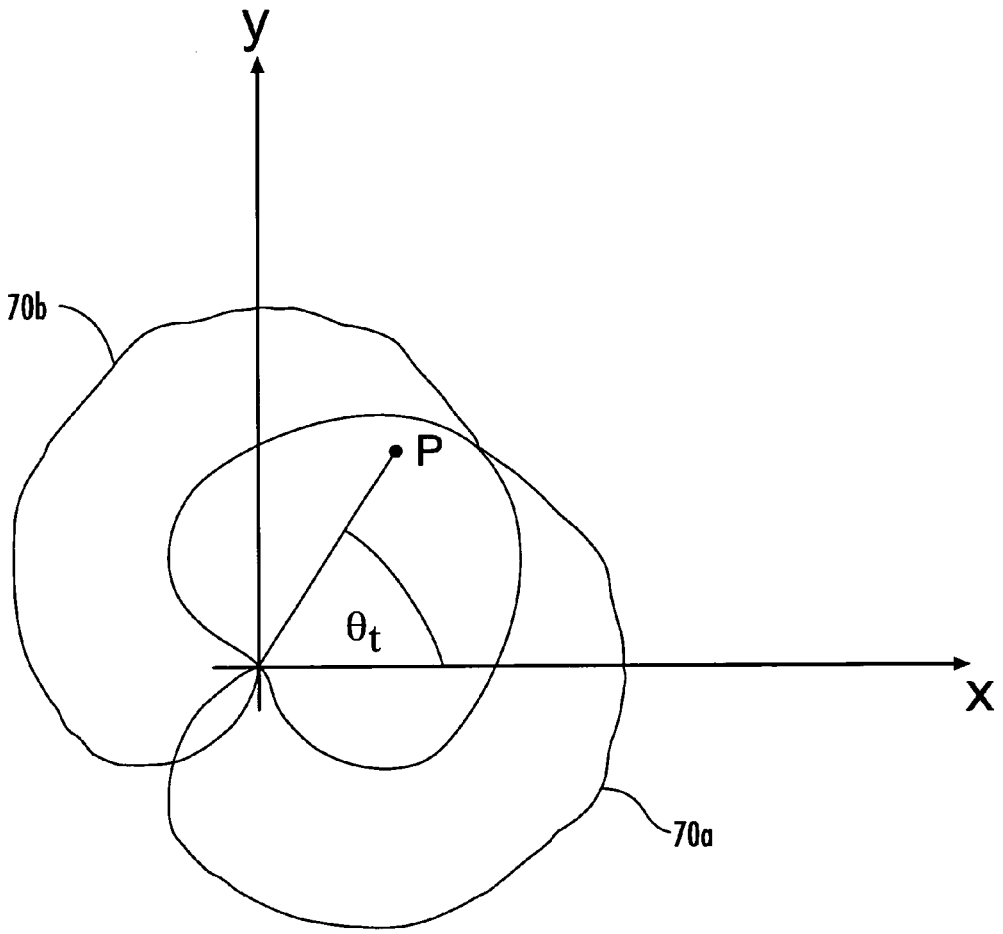


FIG. 8

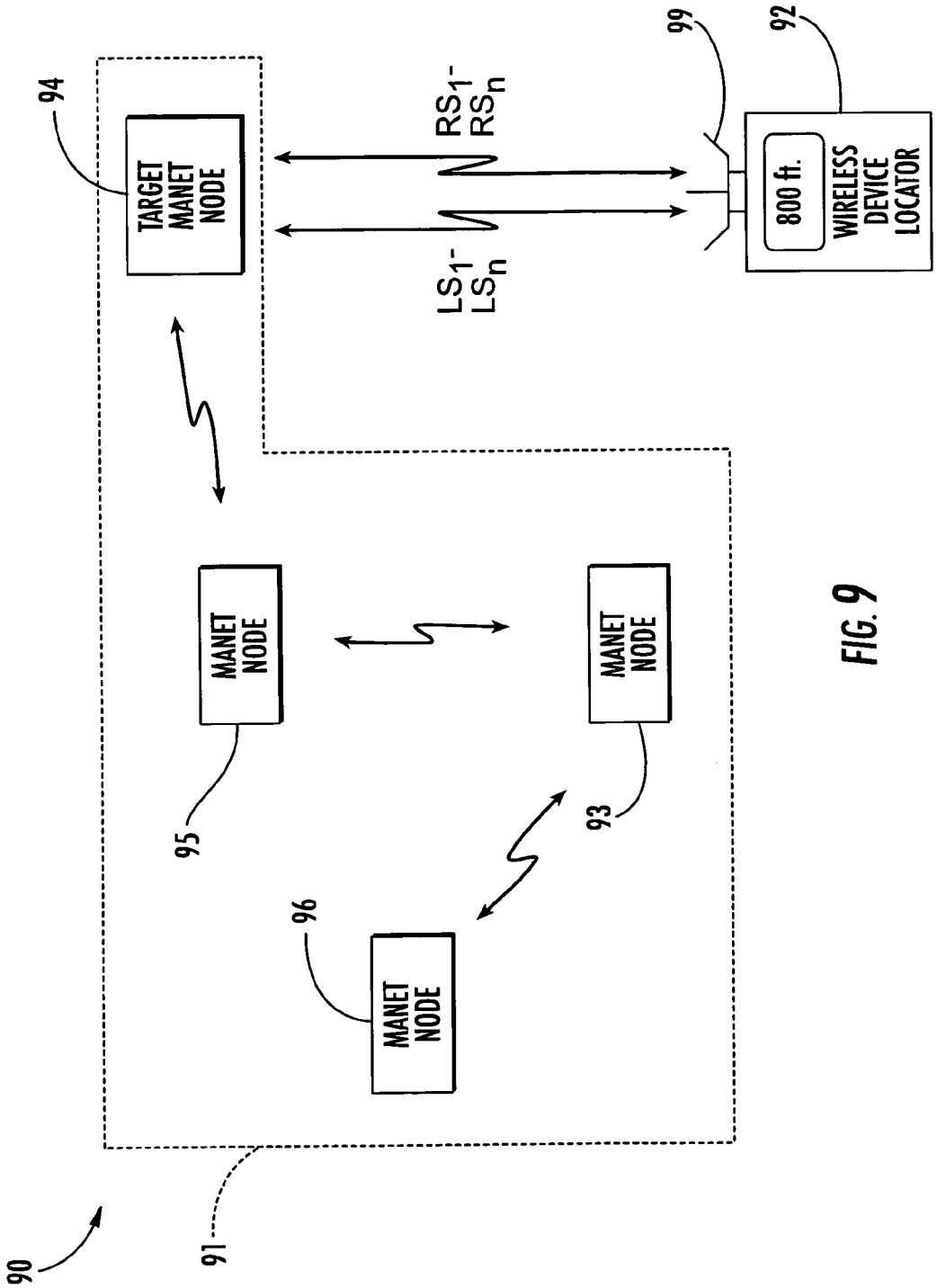

90
91
94
TARGET MANET NODE
95
MANET NODE
96
MANET NODE
93
MANET NODE
LS1-LSn
RS1-RSn
99
92
800 ft.
WIRELESS DEVICE LOCATOR

FIG. 9

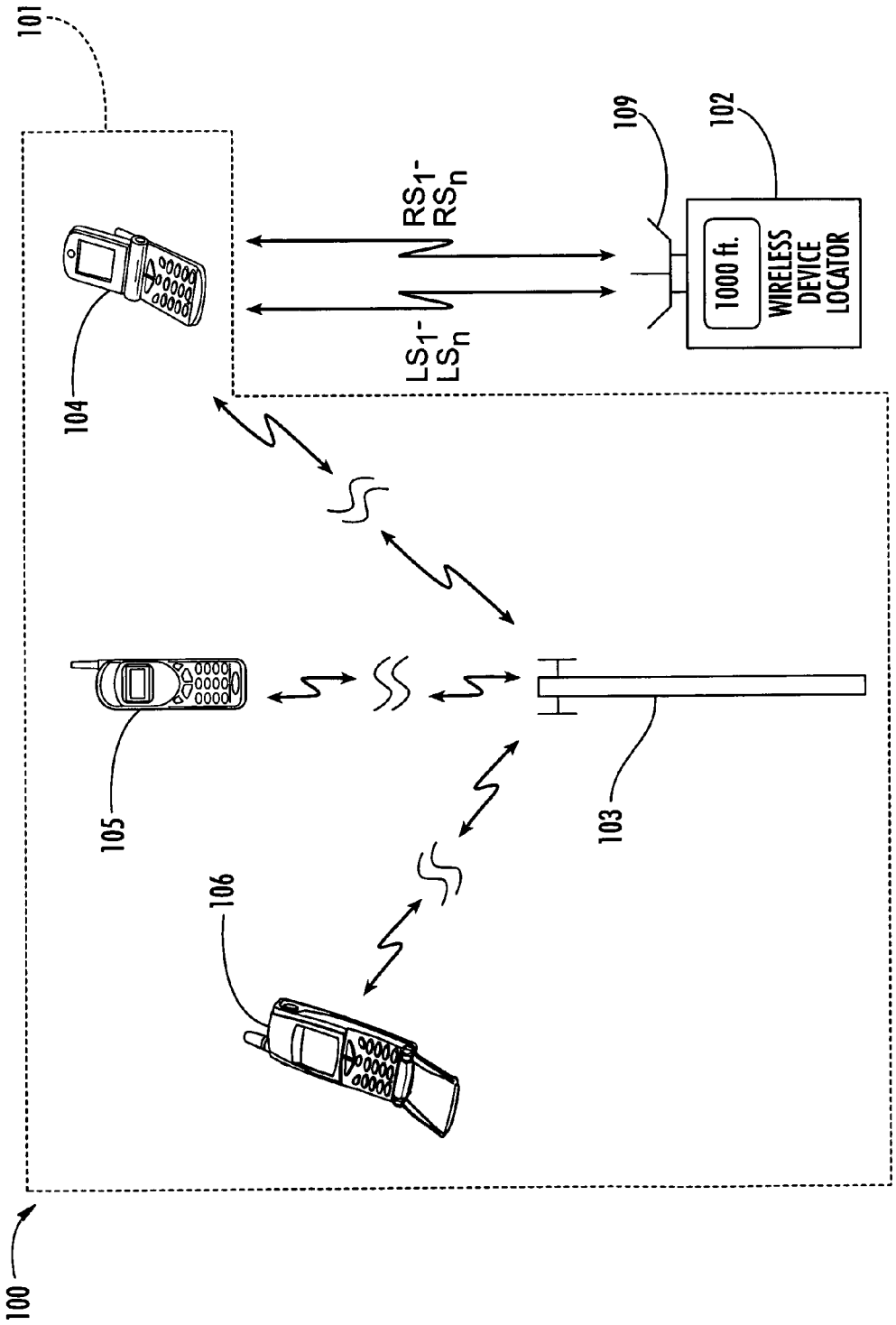

100
101
102
103
104
105
106
109
RS1-RSn
LS1-LSn
1000 ft.
WIRELESS DEVICE LOCATOR

FIG. 10

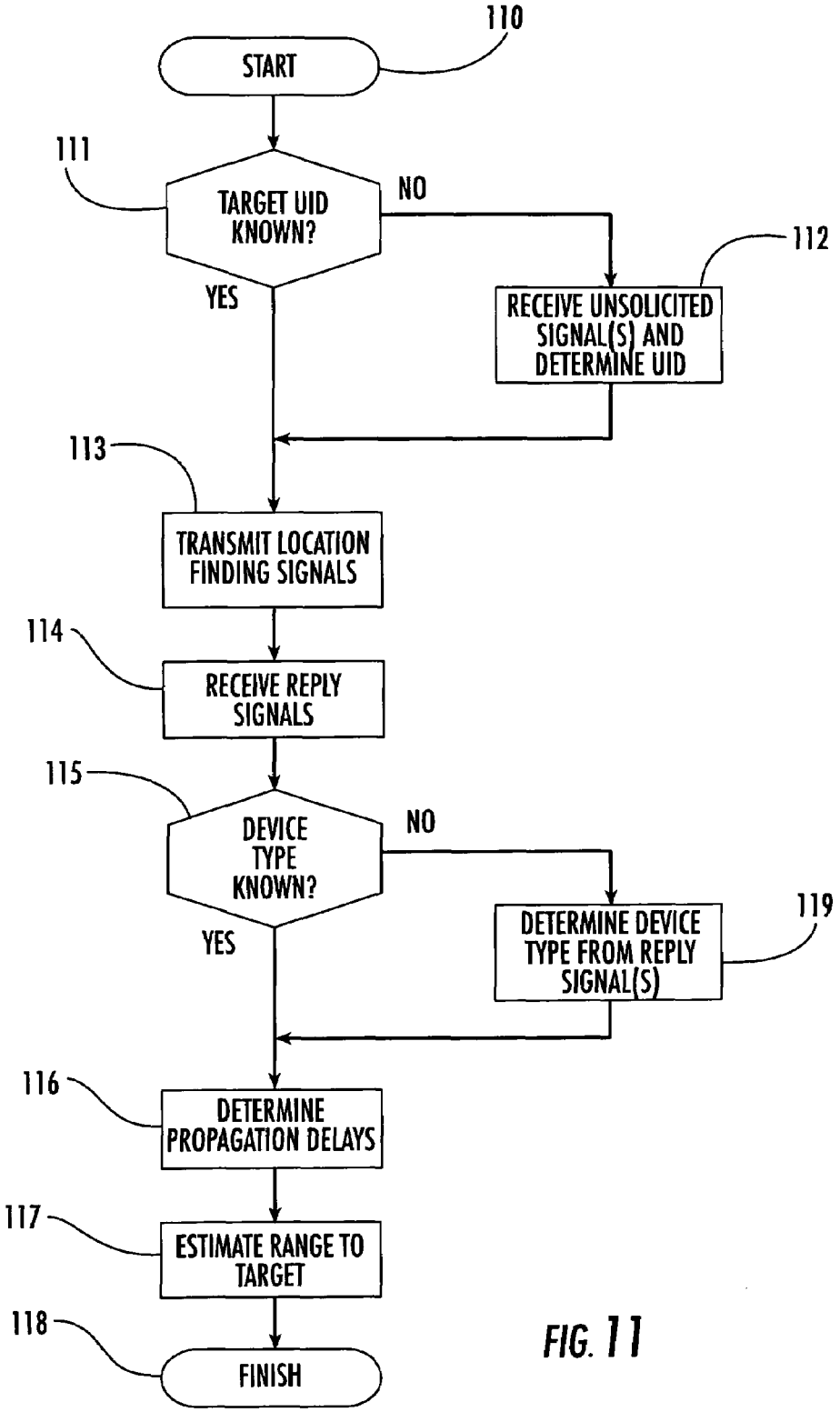

110
START
111
TARGET UID KNOWN?
NO
YES
112
RECEIVE UNSOLICITED SIGNAL(S) AND DETERMINE UID
113
TRANSMIT LOCATION FINDING SIGNALS
114
RECEIVE REPLY SIGNALS
115
DEVICE TYPE KNOWN?
NO
YES
119
DETERMINE DEVICE TYPE FROM REPLY SIGNAL(S)
116
DETERMINE PROPAGATION DELAYS
117
ESTIMATE RANGE TO TARGET
118
FINISH

FIG. 11

WIRELESS COMMUNICATIONS SYSTEM INCLUDING A WIRELESS DEVICE LOCATOR AND RELATED METHODS

FIELD OF THE INVENTION

The present invention relates to the field of wireless communications systems, and, more particularly, to wireless location devices and related methods.

BACKGROUND OF THE INVENTION

Wireless location techniques are used in numerous applications. Perhaps the most basic of these applications is for locating lost articles. By way of example, published U.S. patent application No. 2003/0034887 to Crabtree et al. discloses a portable article locator system for locating lost articles such as glasses, keys, pets, television remotes, etc. More particularly, a wireless transceiver is attached to a person, animal, or other object. A handheld locator transmits a locator signal to the wireless transceiver which includes a unique address code of the transceiver. If the received code matches that stored by the wireless transceiver, it sends a return signal back to the locator device. The locator device uses the return signal to determine the distance and/or direction to the wireless transceiver from the user's location.

The locator device includes an antenna array which includes a plurality of omni-directional antennas. The locator unit determines the bearing to the wireless transceiver by switching between antennas in the antenna array and using Doppler processing to determine a direction of a wireless signal received from the transceiver. The distance to the wireless transmitter is also determined based upon the reception of the wireless signal at each of the antennas of the antenna array. Furthermore, in one embodiment, which is intended to avoid interference between two or more locators in a common area, a plurality of locator signals may be sent from a locator at a standard repetition rate. The locator's receiver then only listens for responses during predetermined windows following each transmission.

In contrast, in some applications it is desirable to determine the location of an unknown signal transmitter. U.S. Pat. No. 5,706,010 to Franke discloses such a system in which a transmitter locator receives a signal from the unknown signal transmitter and processes the signal to determine a bearing to the unknown signal transmitter. The transmitter locator then sends an interrogating signal to the unknown signal transmitter. Upon receiving the interrogating signal, the unknown signal transmitter heterodynes the interrogation signal with its own carrier signal to generate an intermodulation return signal. A processor of the transmitter locator measures the round-trip transit time from the transmission of the interrogation signal to the reception of the intermodulation return signal. A range to the unknown signal transmitter is then calculated based upon the round-trip transit time.

Still another application in which locating a wireless communications device is often necessary is in cellular telephone networks. That is, it may be necessary to locate particular cellular telephone users for law enforcement or emergency purposes, for example. U.S. Pat. No. 6,292,665 to Hildebrand et al., which is assigned to the present assignee, discloses a method for geolocating a cellular phone initiating a 911 call. A base station transceiver transmits a supervisory audio tone (SAT), which is automatically looped back by the calling cellular phone. Returned SAT signals are correlated with those transmitted to determine the

range of the cellular phone. In addition, incoming signals from the cellular phone, such as the returned SAT signals, are received by a phased array antenna and subjected to angle of arrival processing to determine the direction of the cellular phone relative to the base station. The cellular phone is geolocated based upon the angle of arrival and the range information. A correction factor provided by the manufacturer of a given cellular telephone is used to account for the loopback path delay through the phone.

One additional area in which wireless device location can be important is in wireless networks, such as wireless local area networks (WLANs) or wide area networks (WANs), for example. A typical prior art approach to locating terminals within a WLAN includes locating a plurality of receivers at fixed locations within a building, for example, and then determining (i.e., triangulating) the position of a terminal based upon a signal received therefrom at each of the receivers.

Another prior art approach for wireless terminal location is to use a direction finding (DF) device which includes a directional antenna for receiving signals when pointed in the direction of a transmitting node. An example of a portable DF device for WLANs is the Yellowjacket 802.11a wi-fi analysis system from Berkeley Varitronics. This device uses a passive DF technique, i.e., it does not solicit any signals from a terminal but instead waits for the terminal to transmit signals before it can determine the direction of the transmission.

Despite the advantages of such prior art wireless communications device locators, additional wireless location features may be desirable in various applications.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a wireless communications device locator which provides enhanced location features and related methods.

This and other objects, features, and advantages in accordance with the present invention are provided by a wireless communications system which may include a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types. Further, each device type may have a known device latency associated therewith. The system may also include a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality of wireless communications devices. The target wireless communications device may transmit a respective reply signal for each of the location finding signals.

Additionally, the controller of the wireless device locator may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor. This may be done based upon the known device latency of the target wireless communications device. As such, the controller may estimate a range to the target wireless communications device based upon a plurality of determined propagation delays.

In other words, the wireless device locator advantageously provides active range finding. In other words, the wireless device locator prompts the target wireless commu-

nications device to send reply signals using the location finding signals, rather than passively waiting until the target wireless communications device begins transmitting. This allows for quicker and more efficient device location.

Furthermore, by estimating the range based upon a plurality of propagation delays, the wireless device locator mitigates the effects of variations in the device latency time. That is, while the target wireless communication device has a known device latency, there will necessarily be some amount of variance from one transmission to the next. Using a plurality of propagation delays associated with different transmissions provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller may estimate the range based upon an average (e.g., mean, median, mode, etc.) of the propagation delays.

In addition, each wireless communications device may have a unique identifier (UID) associated therewith, and the controller may insert the UID for the target wireless communications device in each of the location finding signals. Furthermore, the target wireless communications device may generate respective reply signals based upon the UID in the location finding signals. That is, the target wireless communications device will act upon the location finding signals because these signals include its UID, whereas the other wireless communications device will not.

The target wireless communications device may generate unsolicited signals including the UID thereof. As such, the controller may cooperate with the transceiver to receive at least one unsolicited signal from the target device, and the controller may also determine the UID for the target device from the at least one unsolicited signal. Thus, if the UID of a target wireless communications device is not already known, the wireless device locator may passively "listen" for unsolicited signals therefrom (i.e., signals that the wireless communications device did not solicit) and determine the UID based thereon.

Additionally, the controller may also determine the device type of the target wireless communications device based upon the UID. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. Accordingly, the controller may determine the device type of the target wireless communications device based upon the MAC address in some applications.

In accordance with another advantageous aspect of the invention, the at least one antenna may be a plurality of antennas, and the controller may cooperate with the plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals. More particularly, the bearing may be a three-dimensional bearing, which may be particularly useful for locating wireless communications devices within a multi-story building, for example. In particular, the antenna(s) may be one or more directional antennas, for example. Further, the wireless device locator may further include a portable housing carrying the at least one antenna, the transceiver, and the controller.

The wireless device locator may be used with numerous type of wireless communications device. For example, the wireless communications devices may be wireless local area network (WLAN) devices, mobile ad-hoc network (MANET) devices, and cellular communications devices.

A method aspect of the invention is for locating a target wireless communications device from among a plurality of wireless communications devices, such as those discussed briefly above. The method may include transmitting a plurality of location finding signals to the target wireless communications device, and receiving a respective reply signal for each of the location finding signals therefrom. The method may further include determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device. As such, a range to the target wireless communications device may be estimated based upon a plurality of determined propagation delays.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is schematic block diagram of a wireless communications system in accordance with the present invention including a wireless local area network (WLAN) and wireless device locator for locating WLAN devices thereof.

FIG. **2** is a schematic block diagram generally illustrating the components of the wireless device locator of FIG. **1**.

FIG. **3** is a graph illustrating the signal propagation delay and device latency components used by the controller of FIG. **2** to estimate range.

FIG. **4** is a schematic block diagram illustrating an embodiment of the wireless device locator of FIG. **2** for a WLAN implementation.

FIG. **5** is a schematic block diagram illustrating in greater detail an embodiment of the transceiver of the wireless device locator of FIG. **4**.

FIGS. **6** and **7** are histograms illustrating range estimation test results performed using the wireless device locator of FIG. **4**.

FIG. **8** is a graph illustrating bearing determination in accordance with the present invention.

FIGS. **9** and **10** are schematic block diagrams illustrating alternate embodiments of the wireless communications system of FIG. **1** including a mobile ad-hoc network (MANET) and a cellular network, respectively.

FIG. **11** is a flow diagram illustrating a wireless device location method in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime and multiple prime notation are used to indicate similar elements in different embodiments.

Referring initially to FIGS. **1** and **2**, a wireless communications system **30** illustratively includes a wireless local area network (WLAN) **31** and a wireless location device **32**. The WLAN **31** illustratively includes an access point **33** (e.g., a server) and a plurality of WLAN devices or terminals which communicate therewith wirelessly, such as the laptop computers **34**, **35**, and the desktop computer **36**. Various WLAN protocols may be used in accordance with the present invention for such wireless communications (e.g., IEEE 802.11, Bluetooth, etc.), as will be appreciated by those of skill in the art. Moreover, it will also be appreciated that additional access points and/or other numbers of wireless communications devices may be used, even though only

a few number thereof are shown for clarity of illustration. Further, numerous other types of WLAN enabled wireless communications devices (e.g., personal data assistants, etc.) may also be used, as will be further appreciated by those skilled in the art.

Each wireless communications device **34**–**36** in the WLAN **31** has a device type associated therewith from among a plurality of different device types. More particularly, the device type may signify the particular manufacturer and/or model of a given WLAN card or chip set used therein. In some embodiments, it may also signify the standard the device complies with (e.g., IEEE 802.11).

The device type is important in that different device types will have known device latencies associated therewith. For example, different WLAN cards or chip sets will have a certain latency associated with the time they take to process a received signal and generate an acknowledgement reply thereto. These delay times may be fairly consistent across different models from a same manufacturer, or they may vary significantly. Additionally, WLAN protocols such as IEEE 802.11 have a specified interframe spacing associated therewith, as will be appreciated by those skilled in the art. Thus, in circumstances where the interframe spacing requirements are closely adhered to, the latency of a given WLAN card or chip set will be substantially equal to the interframe spacing.

The wireless device locator **32** illustratively includes an antenna **39** and a transceiver **41** connected thereto, as well as a controller **42** connected to the transceiver. These components may conveniently be carried by a portable housing **43** in some embodiments, although they could be implemented in a more stationary embodiment, if desired. In the illustrated example, the antenna **39** is a directional antenna, although omni-directional antennas may also be used, as will be appreciated by those skilled in the art. It will also be appreciated that various antenna/transceiver combinations may be used. As will be discussed further below, more than one antenna may be used in certain embodiments to provide bearing determination capabilities, and separate transceivers may optionally be used for respective antennas, if desired.

Operation of the wireless device locator **32** will now be described with reference to FIG. **3**. The controller **42** cooperates with the transceiver **41** for transmitting a plurality of location finding signals to a target wireless communications device to be located from among the plurality of wireless communications devices. In the present example, the laptop **34** is the target device.

As will be appreciated by those skilled in the art, each WLAN device **34**–**36** in the network **31** will have a unique identifier (UID) associated therewith which is used in signals transmitted between the respective devices and the access point **33**. The UID distinguishes the devices **34**–**36** from one another so that each device only acts upon or responds to signals intended for it, and so the access point **33** knows which device it is receiving signals from.

Depending upon a given implementation, the wireless locator device **32** may or may not know the UID of the target device **34** before hand. For example, in some embodiments the wireless device locator **32** could download the UID from the access point **33** (either wirelessly or over a wired network connection, for example). This may be the case when trying to locate a node in a LAN where the node is already registered with the network. However, if the UID is not known, the wireless device locator **32** may passively listen to the target device **34** for unsolicited signals being transmitted therefrom. This feature may be advantageous for law enforcement applications, or for locating an interfering node that is not registered with a particular network but causes interference therewith, for example. By "unsolicited" signals it is meant that these signals are not solicited by the wireless device locator **32** itself, although such signals may have been solicited from another source (e.g., the access point **33**).

The controller **42** cooperates with the transceiver **41** to receive one or more of the unsolicited signals, and the controller determines the UID for the target device **34** therefrom. Of course, the method by which the controller **42** determines the UID from the unsolicited signal will depend upon the given implementation, and whether or to what degree such signals are encrypted.

Additionally, the controller **42** may also determine the device type of the target wireless communications device **34** based upon the UID thereof. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. The MAC addresses may be specific to a particular type of device manufacturer, or indicate a particular operational protocol with which the device is operating, as will be appreciated by those skilled in the art. Accordingly, the controller may determine the device type of the target wireless communications device **34** based upon the MAC address thereof in some applications.

As such, to locate the target device **34**, the controller inserts the UID therefor in each of the location finding signals. By way of example, the location finding signal may include the UID of the target device **34** in a header packet and a valid but empty data packet. This will force the target device **34** to generate a reply signal acknowledging receipt of the location finding signal (i.e., an ACK signal). Of course, various other location finding signals could be used to cause the target terminal **34** to generate an ACK signal, as will be appreciated by those skilled in the art. The controller **42** cooperates with the transceiver **41** for receiving the reply signals from the target device **34** via the antenna **39**. The location finding signals and reply signals may be radio frequency (RF), microwave, optical, or other suitable types of signals, as will be appreciated by those skilled in the art.

The controller **42** determines the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor, and it uses this propagation delay to estimate a range to the target device **34**. However, the propagation delay has to first be determined based upon the total round trip time from the sending of the location finding signal to the reception of the respective reply signal.

The total round trip time will include several components. Referring more particularly to FIG. **3**, the first component is the time associated with transmitting a location finding signal **45**, which is illustrated with an arrow. That is, this is the time from the beginning of the location finding signal transmission (time t_0) to end thereof (time t_1). Two time axes are shown in FIG. **3**. The top or upper axis represents events that occur at the target device **34**, while the bottom or lower axis represents events that occur at the wireless device locator **32**.

The second component of the round trip time is the propagation delay or time t_{PD1} it takes for the location finding signal **45** to travel from the wireless device locator **32** to the target device **34** (i.e., from time t_1 to t_2). The third component of the round trip time is the device latency t_{DL} of the target device **34** (i.e., form time t_2 to t_3). This is the time it takes the target device **34** to receive, process, and transmit a reply signal **46** responsive to the location finding signal **45**. The final components of the round trip time are propagation

delay t_{PD2} of the reply signal **46** (i.e., from time t_3 to t_4), and the reception time thereof by the wireless device locator **32** (i.e., from time t_4 to t_5).

The controller **42** will know the times associated with the transmission of the location finding signal **45** (i.e., from time to t_0 to t_1), as well as the time associated with the reception of the reply signal **46** (i.e., from time t_4 to t_5) for each round trip, since these can be readily measured by the controller. The quantities that the controller **42** will not know are the propagation delays t_{PD1}, t_{PD2} and the actual device latency t_{DL}.

Yet, as noted above, the controller **42** will have access to the known device latency (i.e., a mean latency) for the given device type of the target device **34**, which provides a close approximation of the actual device latency t_{DL}. The known device latency could be a measured value based upon collected data, it could be provided by manufacturers, or it could be based upon a value set in a communications standard, as discussed above, for example.

As will be appreciated by those skilled in the art, the actual device latency will likely vary somewhat from one transmission to the next for any wireless communications device, potentially by as little as a few nanoseconds to a few microseconds, depending upon device configurations, processing loads, etc. Accordingly, a close approximation of the total propagation delay (i.e., time t_{PD1}+time t_{PD2}) may therefore be obtained by substituting the known device latency for the actual device latency t_{DL}, and subtracting this value from the time between times t_1 and t_4. Dividing the total propagation delay by two (since both propagation delays may be considered equal or substantially equal for a stationary or relatively slow moving target device **34**) and multiplying this by the speed of light gives the estimated distance to the target device **39**, based upon the single propagation delay associated with the signal pair **45**, **46**.

Yet, as noted above, device latencies tend to vary from one transmission to the next. Since the location finding signals and reply signals are traveling at the speed of light, such variances can make a significant difference in the estimated distances. More particularly, light travels approximately 1000 ft. in one microsecond. Thus, if the device latency varies by one microsecond from one transmission to the next, the estimated distance to the target device **34** would similarly vary by 1000 ft. or so, which likely will be an unacceptable accuracy for many applications.

In accordance with the present invention, the controller **42** advantageously estimates the range to the target device **34** not solely based upon a single measured propagation delay, but rather upon a plurality thereof. More particularly, by estimating the range based upon a plurality of propagation delays, the wireless device locator **32** mitigates the effects of the variations in the actual device latency time. This provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller **42** may estimate the range based upon an average of the propagation delays, though other suitable statistical functions may also be used (e.g., mean, median, mode, etc.). Of course, it should be noted that the average may be taken on the entire round trip delay instead of first subtracting out the known device latency as described above. That is, the same result may be obtained by first taking the average and then subtracting out the known device latency, as will be appreciated by those skilled in the art.

An exemplary embodiment of the present invention is now described with reference to FIGS. **4** and **5**. The wireless device locator **32'** may use a personal data assistant (PDA) as the controller **42'**, although a personal computer (PC) or other suitable computing device may also be used. More particularly, the PDA **42'** illustratively includes a graphical user interface (GUI) **50'**, and a received signal strength indication (RSSI) processing module **51'** for cooperating with the transceiver **41'** to perform above-described range estimation processing operations. More particularly, the RSSI module **51'** may be implemented as a software module which is run on the PDA **42'**, as will be appreciated by those skilled in the art, and which cooperates with the GUI to provide range estimates to a user.

The PDA **50'** also illustratively includes a battery **52'**, which may conveniently be used for powering the various transceiver **41'** components, as shown. Of course, it will be appreciated that separate batteries may be used, or one or more components of the wireless device locator **32'** may be powered by an external (e.g., AC) source. The transceiver **41'** operates in accordance with the IEEE 802.11b standard and includes a MAC-less 802.11b radio **58'** and a field-programmable gate array (FPGA) **53'** connected thereto. The FPGA **53'** illustratively includes a packet building module **54'**, a radio configuration module **55'**, a receiver filtering module **56'**, and a simple MAC processing module **57'** for processing the location finding signals and reply signals and communicating with the radio **53'** in accordance with the 802.11b standard, as will be appreciated by those skilled in the art.

More specifically, the MAC-less radio **58'** may be a GINA model RF module from GRE America, Inc., and the FPGA **53'** may be a module EPXA10 from Altera Corp. The hardware components of the FPGA **53"** illustratively include an ARM922T processor **60"**, block RAM **61"** therefor, a serial/universal serial bus (USB) interface **62"**, and a programmable logic section **63"**. Additional circuitry including an oscillator **64"**, power management circuitry (i.e., regulators, microprocessor supervisor, etc.) **65"**, and a programmable read-only memory (PROM)/boot flash memory **66"** are connected thereto as shown, as will be appreciated by those skilled in the art.

Referring now to FIGS. **6**–**7**, a test was conducted in accordance with the present invention in which approximately 1500 location finding signals were transmitted to a stationary wireless IEEE 802.11 device. The time it took to receive the reply signal was measured by ticks of an internal clock of the controller **42**, where each tick represents 7.567 ns. From FIG. **6** it may be seen that the reply signals from the target device were returned within between about 20,960 and 21,045 clock ticks, where the transmission of the respective location signals each began at 0 clock ticks. Moreover, if this range is divided into equal sections or bins, the frequency (i.e., number) of round trip times that fell within each of the bins is shown in FIG. **7**.

Plotting various statistical functions of the measured clock tick samples (such as the mean and the mode) versus the known distance to the target device allowed statistical curve-fitting to take place, as shown in FIG. **6**. It was determined from the test results that taking the mean of the samples provided the most accurate range estimation. More particularly, the ranges to several 802.11b target devices at varying distances were estimated using this approach, and the worst case error for the estimated range was never more than 20 ft. Preferably, the location finding signals are transmitted over a relatively short interval (a few seconds or less) so that if the target device is moving the accuracy of the results will not be significantly diminished. Of course, various numbers of location finding signals and transmission

intervals may be used depending upon the particular implementation, as will be appreciated by those skilled in the art.

In accordance with another advantageous aspect of the invention, multiple antennas **39***a*", **39***b*" (FIG. **5**) may be used to provide target bearing in addition to the estimated range. Referring more particularly to FIG. **8**, bearing determination in the case where the antennas **39***a*", **39***b*" are directional antennas will now be described. The antennas **39***a*", **39***b*" have respective reception patterns **70***a*, **70***b*, which may be orthogonal to one another (i.e., the former is directed along the x-axis, while the latter is directed along the y-axis).

The target device is at a point P, which is within the reception patterns **70***a*, **70***b*. Each of the antenna gain patterns **70***a* and **70***b* can be measured and known to the locator, and represented by gain functions G**1**(θ) and G**2**(θ) where θ represents the angle of deviation from a particular reference direction.

As such, to determine the line of bearing to the target device, the received signal strength is measured from each of the antennas **70***a*, **70***b*, respectively. Based upon this information, the controller **42'** may then find the angle θ_t using the relationship $G1(\theta_t)-G2(\theta_t)=P1-P2$, where P**1** and P**2** is the received signal power off antenna **1** and antenna **2**, respectively. In other words, the difference in the signal strength received between the two antennas (P**1**−P**2**) should equal the difference in the antenna gain of the two antennas at the angle of the line of bearing $(G1(\theta_t)-G2(\theta_t))$ Thus, the target line of bearing to the target device is at θ_t. It should be noted that it is possible that more than one angle θ may satisfy the relationship $G1(\theta_t)-G2(\theta_t)=P1-P2$. These multiple angles represent a line of bearing ambiguity that can easily be resolved by making multiple measurements, as can be appreciated by those skilled in the art.

As noted above, more than one transceiver **41'** may be used in certain embodiments, which would allow signal strength measurements to be taken based upon a same reply signal from the target device. However, if only a single transceiver **41'** is used, the controller **42'** may alternate which antenna **70***a*, **70***b* is receiving and measure the received signal strength of successive signals, for example. Moreover, the bearing may be determined in three dimensions, if desired, which may be particularly useful for locating wireless communications devices within a multistory building, for example, as will be appreciated by those skilled in the art.

While the present invention has been described above with reference to a WLAN wireless device locator **32'**, it will be appreciated by those skilled in the art that it may also be used in other wireless communications systems with other types of wireless communications devices. Referring more particularly to FIG. **9**, a mobile ad-hoc network (MANET) system **90** illustratively includes a wireless device locator **92** including an antenna **99**, such as those described above, and a MANET **91**. More particularly, the MANET includes MANET nodes or devices **93**–**96**, of which the node **94** is the target node in the illustrated example. Here, the wireless device locator **92** performs range and/or bearing estimation in the same manner described above, except that it will operate in accordance with the appropriate MANET protocol used within the system **90**, as will be appreciated by those skilled in the art.

Another embodiment is illustrated in FIG. **10**, in which a wireless device locator **102** having an antenna **109** is used within a cellular communications system **100** for locating cellular devices (e.g., cellular telephones) **104**–**106** in cellular network **101**. The cellular devices **104**–**106** place and receive calls via a cellar tower **103**, as will be appreciated by those skilled in the art. In the illustrated example, the target device is the cell phone **104**. Here again, the wireless device locator **102** will communicate using the appropriate operating protocol being used in the cellular network **101** (e.g., code-division multiple access (CDMA), short message service (SMS), etc.), as will be appreciated by those skilled in the art.

Turning now additionally to FIG. **11**, a method aspect of the invention is for locating a target wireless communications **34** device from among a plurality of wireless communications devices **34**–**36**. Beginning at Block **110**, if the UID for the target device **34** is unknown, the controller **42** may determine the UID from unsolicited signals transmitted by the target device, for example, as described above (Block **112**). Of course, in some embodiments, the controller **42** may download the signals from a network access point **33**, etc., as also described above.

Once the UID for the target wireless communication device **34** is known, location finding signals are transmitted to the target wireless communications device, at Block **113**, and respective reply signals for each of the location finding signals are received therefrom, at Block **114**. If the device type (and, thus, the known device latency) are known, at Block **115**, then the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor is determined based upon the known device latency of the target wireless communications device **34**, at Block **116**. As such, a range to the target wireless communications device **34** is estimated based upon a plurality of determined propagation delays (Block **117**), as previously discussed above, thus concluding the illustrated method (Block **118**).

Of course, if the device type is unknown, the controller **42** may determine the device type from the reply signal (Block **119**), as discussed above, or by other suitable methods which will be appreciated by those skilled in the art. It should be noted that while this step is shown as occurring after the receipt of the reply signals in the illustrated example, the device type determination may be performed prior thereto, such as while determining the UID, for example.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A wireless communications system comprising:

a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith; and

a wireless device locator comprising

at least one antenna and a transceiver connected thereto, and

a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among said plurality of wireless communications devices and inserting the UID for said target wireless communications device in each of the location finding signals;

said target wireless communications device transmitting a respective reply signal for each of said location finding signals based upon the UID in the location finding signals;

said controller of said wireless device locator also for cooperating with said transceiver for receiving the reply signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target wireless communications device, and

estimating a range to said target wireless communications device based upon a plurality of determined propagation delays.

2. The wireless communications system of claim **1** wherein said controller estimates the range based upon an average of the propagation delays.

3. The wireless communications system of claim **1** wherein said target wireless communications device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from said target device; and wherein said controller determines the UID for said target wireless communications device from the at least one unsolicited signal.

4. The wireless communications system of claim **3** wherein said controller determines the device type of said target wireless communications device based upon the UID thereof.

5. The wireless communications system of claim **4** wherein the UIDs comprise media access control (MAC) addresses of respective wireless communications devices, and wherein said controller determines the device type of said target wireless communications device based upon the MAC address thereof.

6. The wireless communications system of claim **1** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target wireless communications device based upon at least one of the received reply signals.

7. The wireless communications system of claim **6** wherein the bearing is a three-dimensional bearing.

8. The wireless communications system of claim **1** wherein said at least one antenna comprises at least one directional antenna.

9. The wireless communications system of claim **1** wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller.

10. The wireless communications system of claim **1** wherein said wireless communications devices comprise wireless local area network (WLAN) devices.

11. The wireless communications system of claim **1** wherein said wireless communications devices comprise mobile ad-hoc network (MANET) devices.

12. The wireless communications system of claim **1** wherein said wireless communications devices comprise cellular communications devices.

13. A wireless communications system comprising:

a plurality of wireless local area network (WLAN) devices each having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith; and

a wireless device locator comprising

at least one antenna and a transceiver connected thereto, and

a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target WLAN device from among said plurality of WLAN devices and inserting the UID for said target wireless communications device in each of the location finding signals;

said target WLAN device transmitting a respective reply signal for each of said location finding signals based upon the UID in the location finding signals;

said controller of said wireless device locator also for

cooperating with said transceiver for receiving the reply signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target WLAN device, and

estimating a range to said target WLAN device based upon an average of a plurality of determined propagation delays.

14. The wireless communications system of claim **13** wherein said target WLAN device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from said target WLAN device; and wherein said controller determines the UID for said target WLAN device from the at least one unsolicited signal.

15. The wireless communications system of claim **14** wherein said controller determines the device type of said target WLAN device based upon the UID thereof.

16. The wireless communications system of claim **15** wherein the UIDs comprise media access control (MAC) addresses of respective WLAN devices, and wherein said controller determines the device type of said target WLAN device based upon the MAC address thereof.

17. The wireless communications system of claim **13** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target WLAN device based upon at least one of the received reply signals.

18. A wireless device locator for locating a target wireless communications device having a unique identifier (UID) associated therewith, the wireless device locator comprising:

at least one antenna and a transceiver connected thereto; and a controller for

cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device, inserting the UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of said location finding signals generated by the target wireless communications device based upon the UID in the location finding signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device, and

estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

19. The wireless device locator of claim **18** wherein said controller estimates the range based upon an average of the propagation delays.

20. The wireless device locator of claim **18** wherein the target wireless communications device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from the target device; and wherein said controller determines the UID for the target wireless communications device from the at least one unsolicited signal.

21. The wireless device locator of claim **18** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals.

22. The wireless device locator of claim **18** wherein said at least one antenna comprises at least one directional antenna.

23. The wireless device locator of claim **18** wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller.

24. The wireless device locator of claim **18** wherein the target wireless communications device comprises a wireless local area network (WLAN) device.

25. The wireless device locator of claim **18** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

26. The wireless device locator of claim **18** wherein the target wireless communications device comprises a cellular communications device.

27. A method for locating a target wireless communications device from among a plurality of wireless communications devices, each wireless communications device having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith, the method comprising:

transmitting a plurality of location finding signals to the target wireless communications device, inserting the UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of the location finding signals generated by the target wireless communications device based upon the UID in the locations signals;

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device; and estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

28. The method of claim **27** wherein the controller estimates the range based upon an average of the propagation delays.

29. The method of claim **27** wherein the target wireless communications device generates unsolicited signals including the UID thereof; and further comprising:

receiving at least one unsolicited signal from the target device; and

determining the UID for the target wireless communications device from the at least one unsolicited signal.

30. The method of claim **29** further comprising determining the device type of the target wireless communications device based upon the UID thereof.

31. The method of claim **27** further comprising determining a bearing to the target wireless communications device based upon at least one of the received reply signals.

32. The method of claim **27** wherein the target wireless communications device comprises a wireless local area network (WLAN) device.

33. The method of claim **27** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

34. The method of claim **27** wherein the target wireless communications device comprises a cellular communications device.

* * * * *

Exhibit 3

US007321777B2

(12) **United States Patent**
Billhartz et al.

(10) **Patent No.: US 7,321,777 B2**
(45) **Date of Patent: *Jan. 22, 2008**

(54) **WIRELESS COMMUNICATIONS SYSTEM INCLUDING A WIRELESS DEVICE LOCATOR AND RELATED METHODS**

(75) Inventors: **Thomas Jay Billhartz**, Melbourne, FL (US); **Vivek Krishna**, Palm Bay, FL (US); **Steve Kopman**, Melbourne, FL (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/531,487**

(22) Filed: **Sep. 13, 2006**

(65) **Prior Publication Data**

US 2007/0026873 A1 Feb. 1, 2007

Related U.S. Application Data

(63) Continuation of application No. 10/767,794, filed on Jan. 29, 2004, now Pat. No. 7,110,779.

(51) **Int. Cl.**
H04Q 7/20 (2006.01)

(52) **U.S. Cl.** **455/456.2**; 455/456.1; 455/456.5; 455/456.6; 342/457; 370/328

(58) **Field of Classification Search** 455/41.2–41.3, 455/456.1–457, 553.1, 63.4, 562.1, 67.11, 455/67.13, 67.16, 402.2; 342/357.08–357.09, 342/357.1, 450; 340/426.19, 426.22, 539.23, 340/825.49; 370/310.2, 328, 331, 338; 701/201; 702/149

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,526,357	A	6/1996	Jandrell	370/95.2
5,550,549	A	8/1996	Procter, Jr. et al.	342/47
5,687,196	A	11/1997	Proctor, Jr. et al.	375/347
5,706,010	A	1/1998	Franke	342/47
6,292,665	B1	9/2001	Hildebrand et al.	455/456
6,680,923	B1	1/2004	Leon	370/328
6,865,394	B2	3/2005	Ogino et al.	455/456.1

(Continued)

OTHER PUBLICATIONS

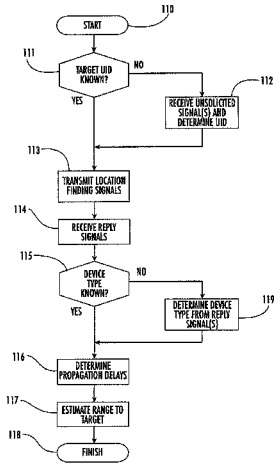
Yellowjacket-A, 802.11a Wi-Fi Analysis System, Berkeley Varitronics Systems.

Primary Examiner—George Eng
Assistant Examiner—Kamran Afshar
(74) *Attorney, Agent, or Firm*—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A wireless communications system may include a plurality of wireless communications devices and a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality thereof. The target device may transmit a respective reply signal for each of the location finding signals. Additionally, the controller may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target device. As such, the controller may estimate a range to the target device based upon a plurality of determined propagation delays.

25 Claims, 9 Drawing Sheets



U.S. PATENT DOCUMENTS

6,990,428	B1 *	1/2006	Kaiser et al.	455/456.1
7,042,868	B2 *	5/2006	Runkle et al.	370/347
7,046,987	B2 *	5/2006	Siegel et al.	455/404.2
7,110,779	B2 *	9/2006	Billhartz et al.	455/456.2
2002/0080759	A1	6/2002	Harrington et al.	370/338
2002/0118655	A1	8/2002	Harrington et al.	370/328
2002/0171586	A1	11/2002	Martorana et al.	342/458
2003/0025602	A1	2/2003	Medema et al.	340/568.1
2003/0034887	A1	2/2003	Crabtree et al.	340/539
2003/0043073	A1	3/2003	Gray et al.	342/465
2003/0117320	A1 *	6/2003	Kim et al.	342/457
2003/0128163	A1 *	7/2003	Mizugaki et al.	342/464
2003/0162550	A1	8/2003	Kuwahara et al.	455/456
2003/0182062	A1	9/2003	DeLorne et al.	701/201
2003/0191604	A1	10/2003	Kuwahara et al.	702/150
2004/0072566	A1 *	4/2004	Kuwahara et al.	455/440
2004/0081139	A1	4/2004	Beckmann et al.	370/352
2004/0110514	A1	6/2004	Kim et al.	455/456.1
2004/0203889	A1	10/2004	Karaoguz	455/456.1
2004/0266348	A1	12/2004	Deshpande et al.	455/41.2
2005/0037775	A1	2/2005	Moeglein et al.	455/456.1
2005/0059411	A1	3/2005	Zhengdi	455/456.1
2006/0183488	A1 *	8/2006	Billhartz	455/456.5

* cited by examiner

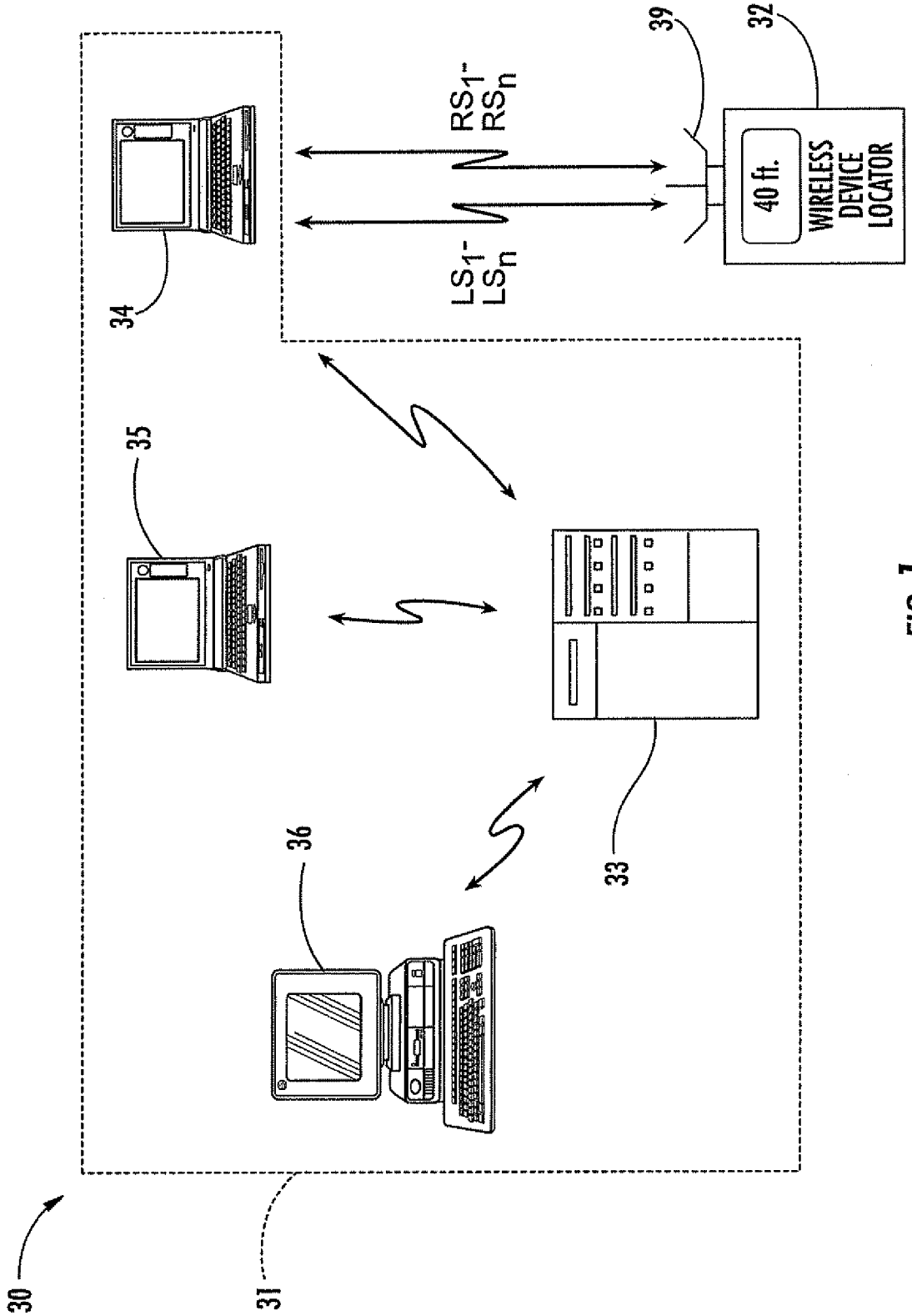

30
31
34
35
36
33
39
32
RS1-
RSn
LS1-
LSn
40 ft.
WIRELESS
DEVICE
LOCATOR

FIG. 1

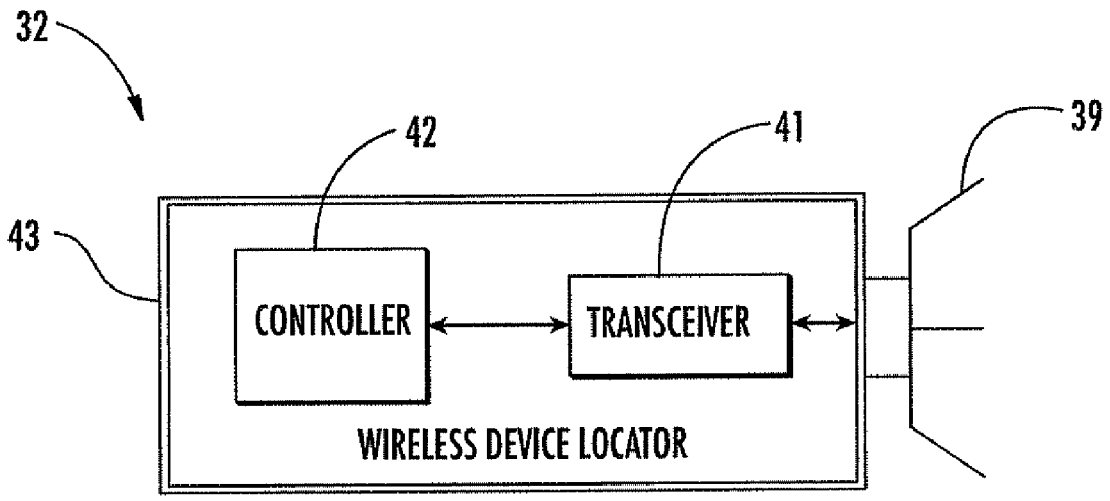

32
42
41
39
43
CONTROLLER
TRANSCEIVER
WIRELESS DEVICE LOCATOR

FIG. 2

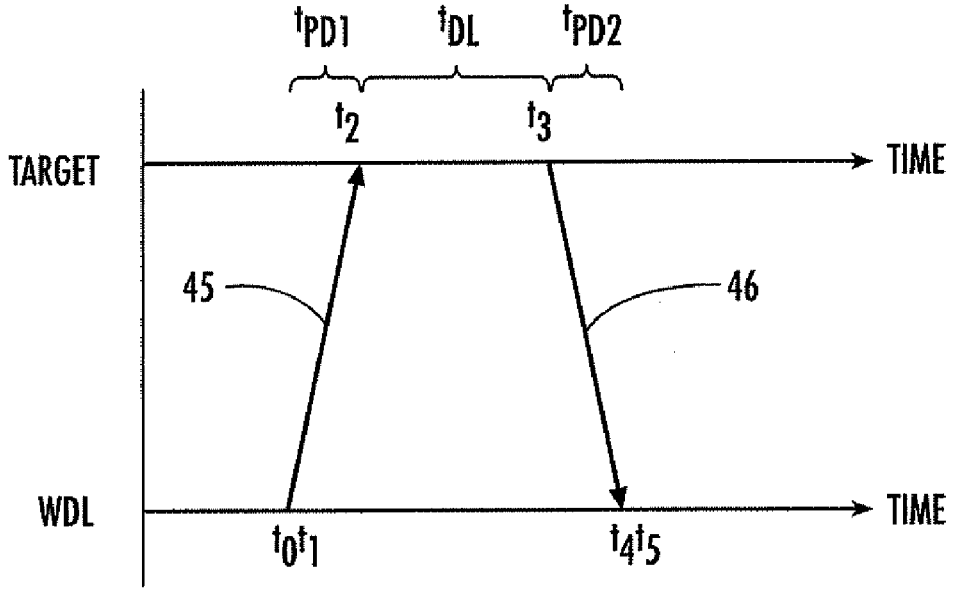

tPD1
tDL
tPD2
t2
t3
TARGET
TIME
45
46
WDL
TIME
t0t1
t4t5

FIG. 3

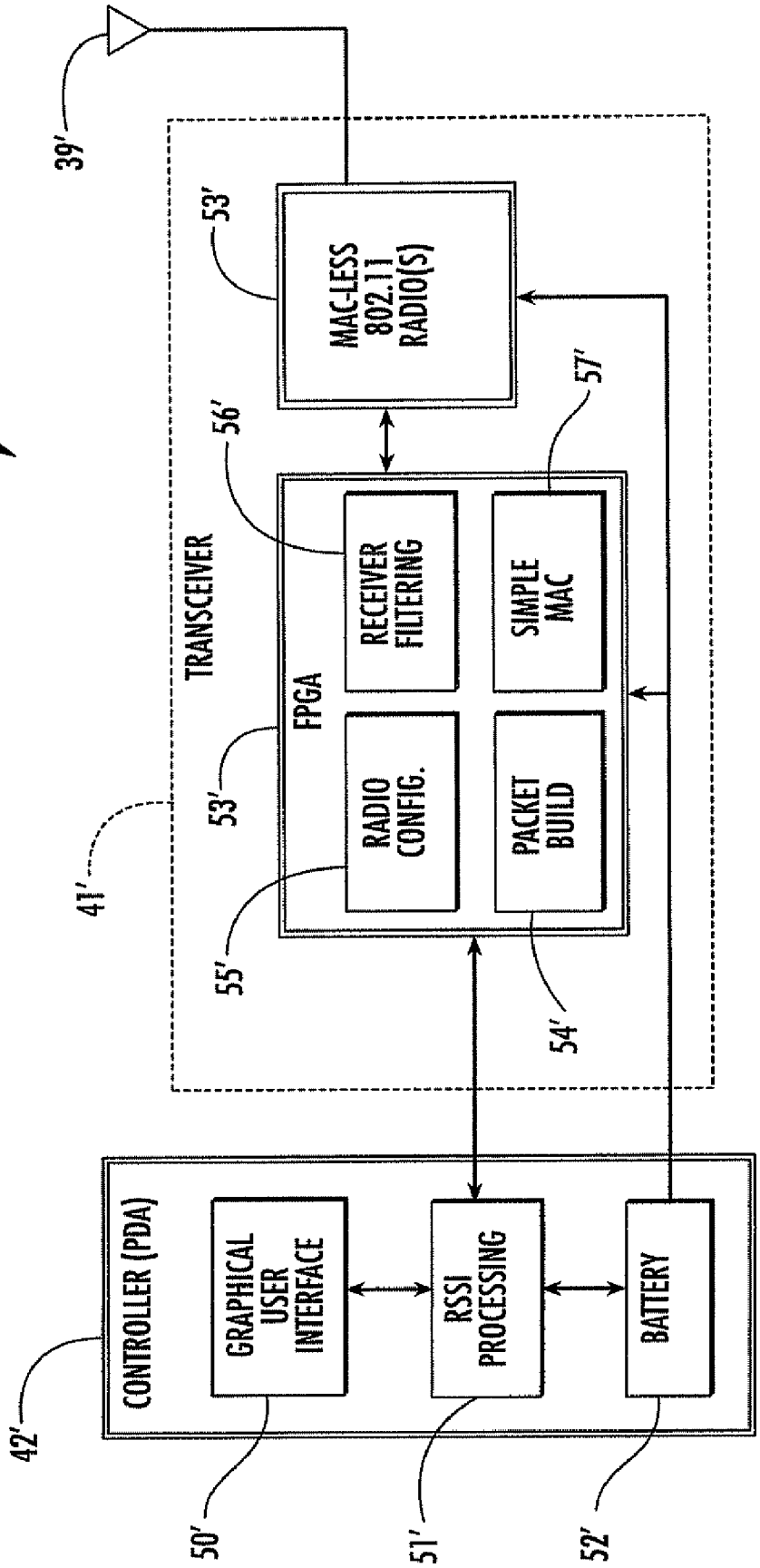

32'
39'
53'
MAC-LESS 802.11 RADIO(S)
56'
57'
TRANSCEIVER
FPGA
RECEIVER FILTERING
SIMPLE MAC
53'
RADIO CONFIG.
PACKET BUILD
41'
55'
54'
CONTROLLER (PDA)
GRAPHICAL USER INTERFACE
RSSI PROCESSING
BATTERY
42'
50'
51'
52'

FIG. 4

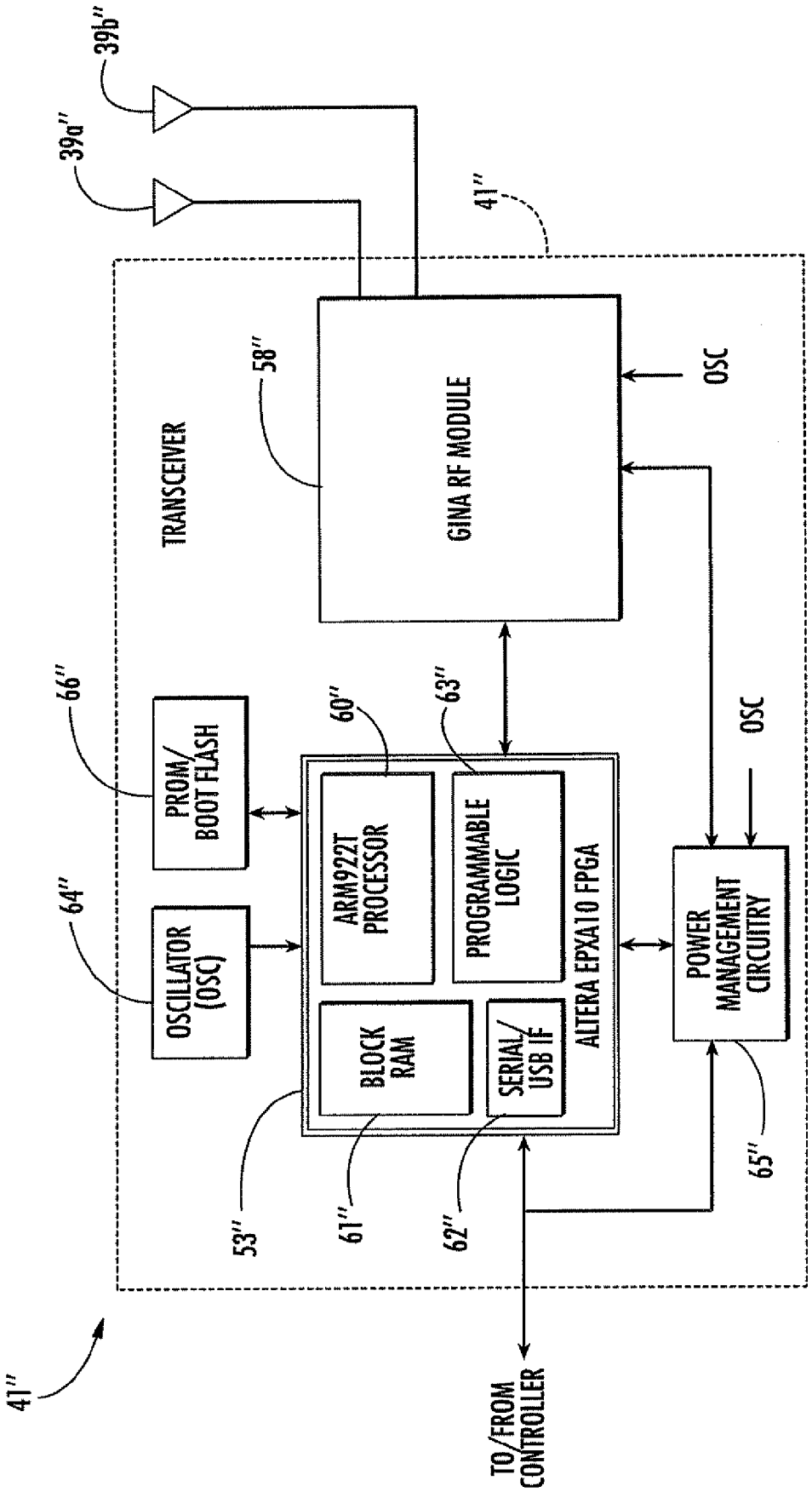

39b''
39a''
41''
TRANSCEIVER
58''
GINA RF MODULE
OSC
66''
PROM/
BOOT FLASH
60''
63''
ARM922T
PROCESSOR
PROGRAMMABLE
LOGIC
ALTERA EPXA10 FPGA
OSC
64''
OSCILLATOR
(OSC)
BLOCK
RAM
SERIAL/
USB IF
POWER
MANAGEMENT
CIRCUITRY
53''
61''
62''
65''
41''
TO/FROM
CONTROLLER

FIG. 5

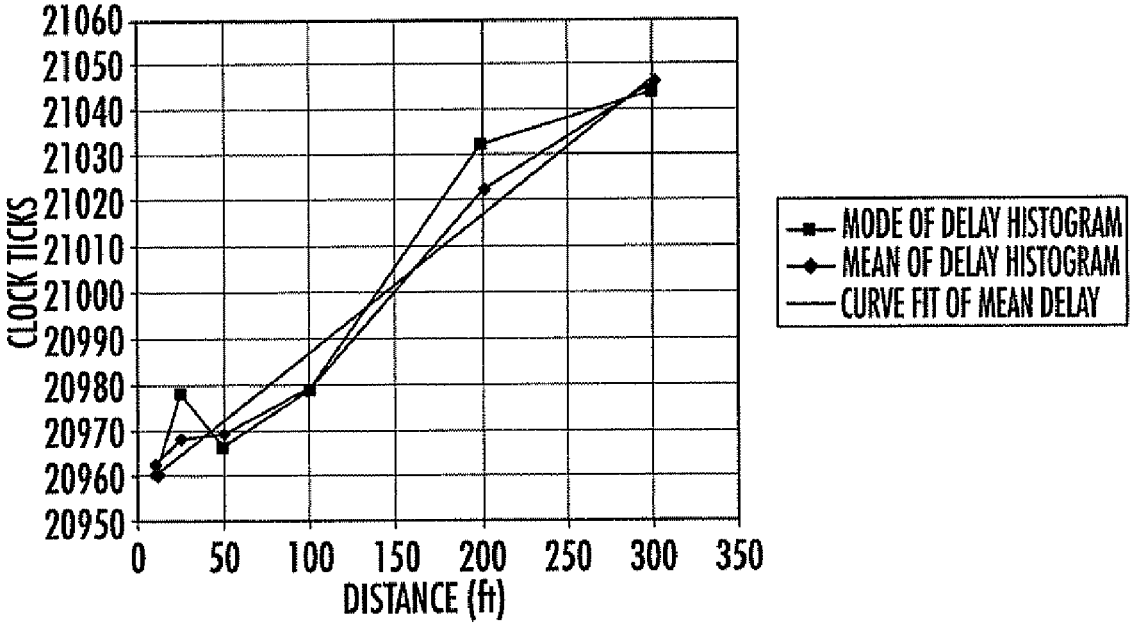

21060
21050
21040
21030
21020
21010
21000
20990
20980
20970
20960
20950
CLOCK TICKS
0
50
100
150
200
250
300
350
DISTANCE (ft)
MODE OF DELAY HISTOGRAM
MEAN OF DELAY HISTOGRAM
CURVE FIT OF MEAN DELAY

FIG. 6

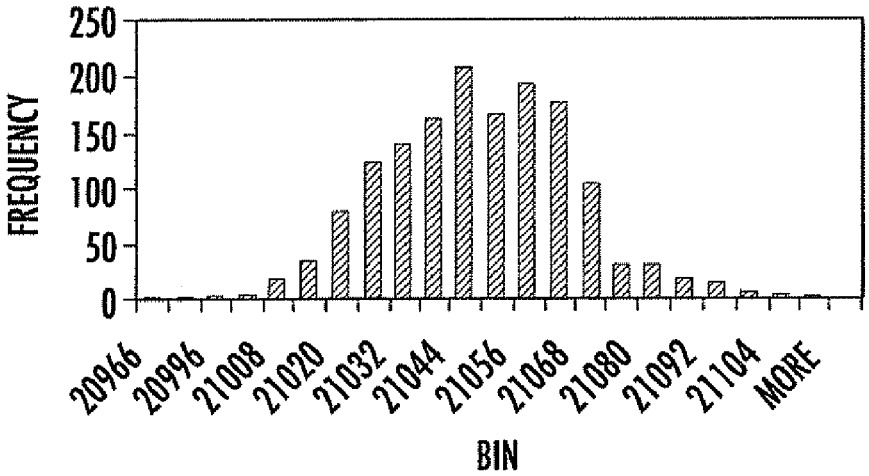

250
200
150
100
50
0
FREQUENCY
20966
20996
21008
21020
21032
21044
21056
21068
21080
21092
21104
MORE
BIN

FIG. 7

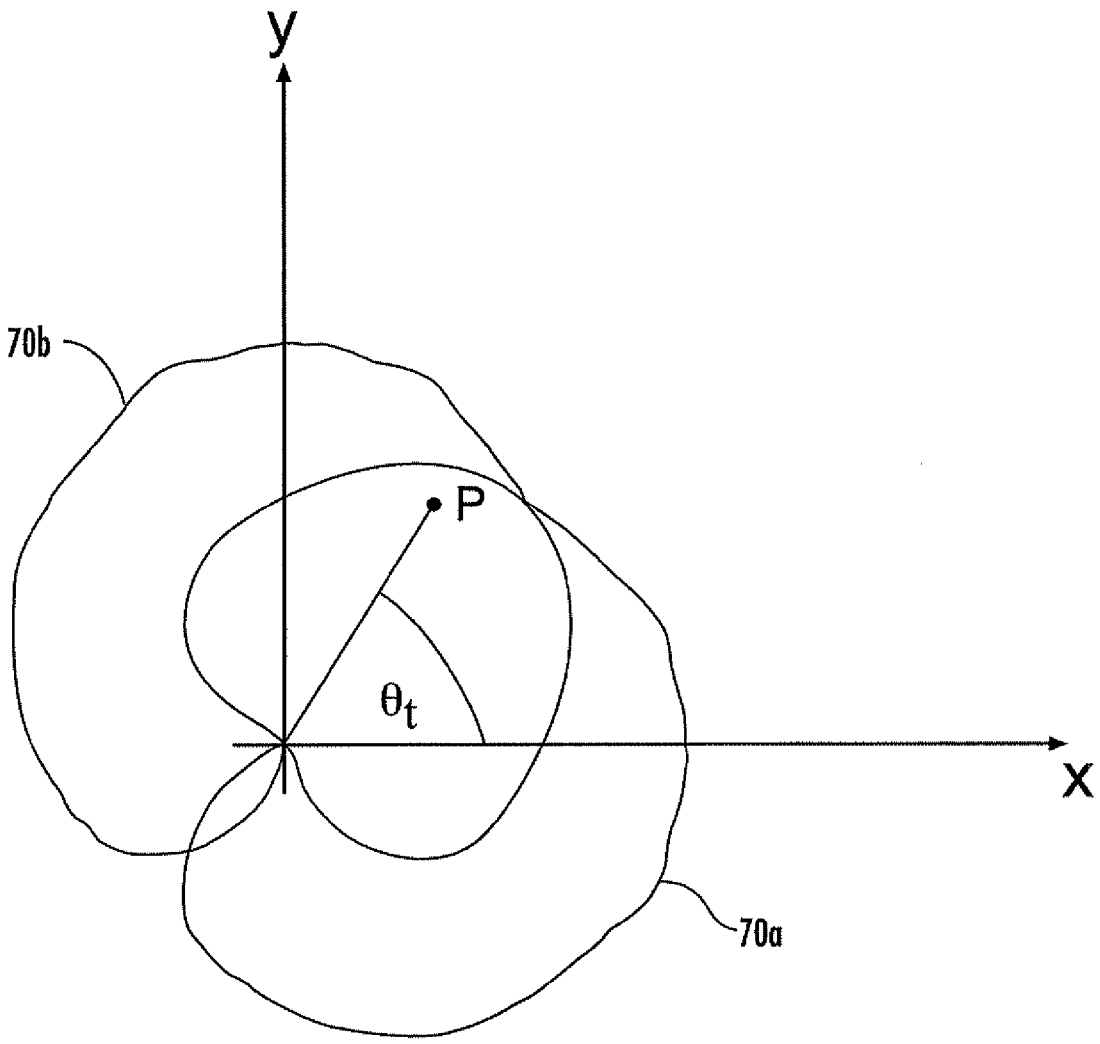


FIG. 8

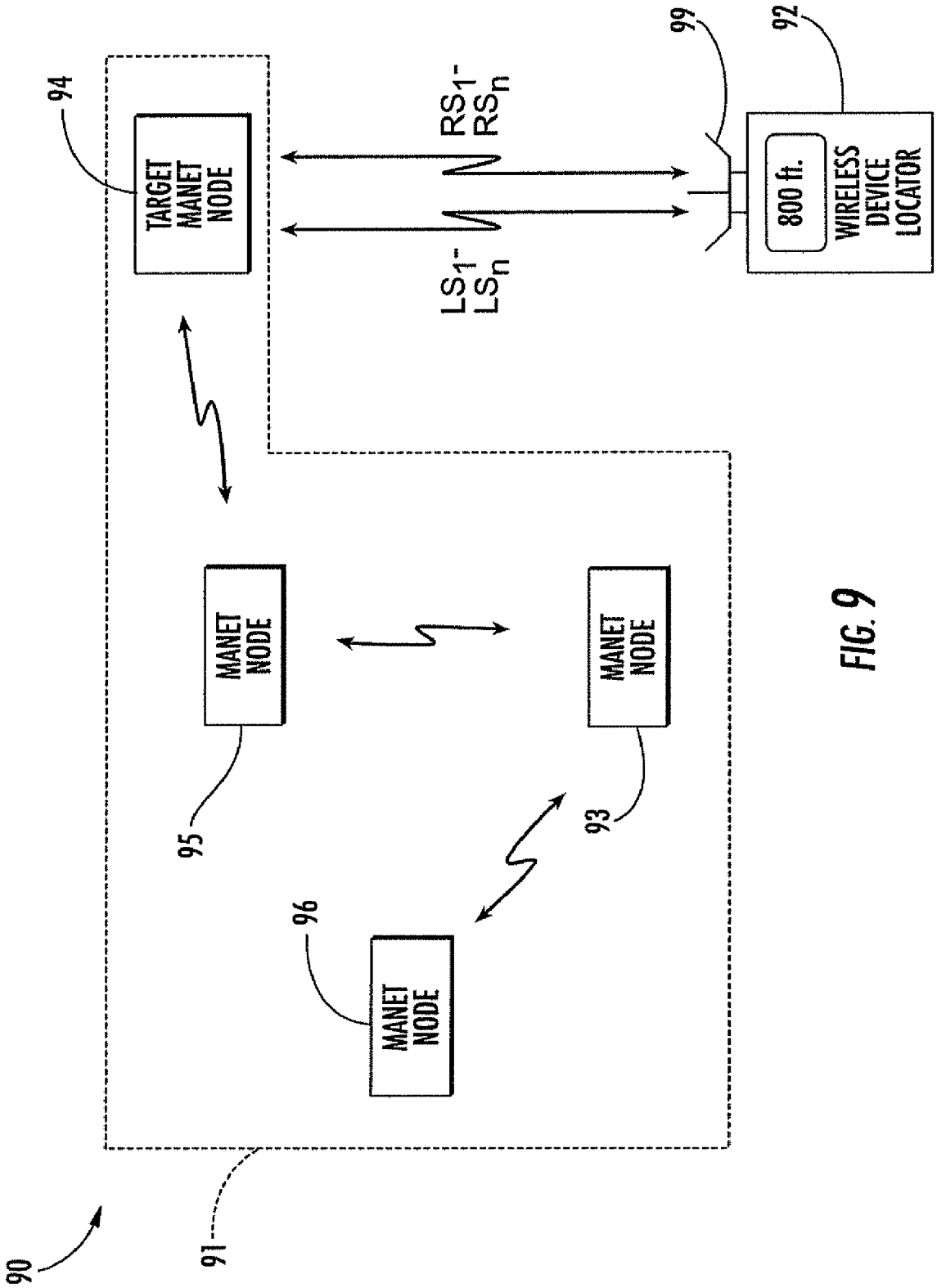

90
91
94
TARGET MANET NODE
95
MANET NODE
96
MANET NODE
93
MANET NODE
LS1-LSn
RS1-RSn
99
92
800 ft.
WIRELESS DEVICE LOCATOR

FIG. 9

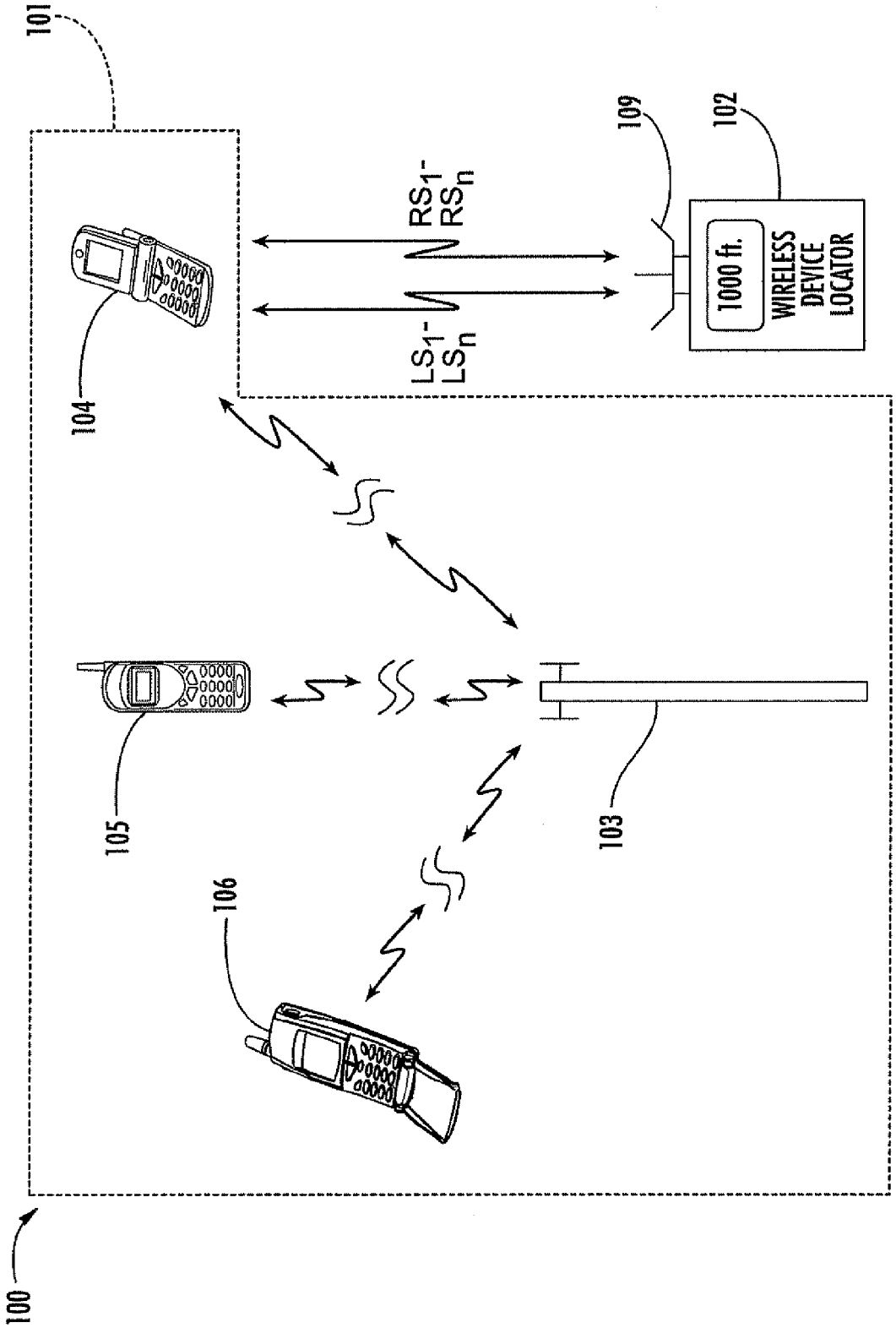

100
101
102
103
104
105
106
109
RS1-RSn
LS1-LSn
1000 ft.
WIRELESS DEVICE LOCATOR

FIG. 10

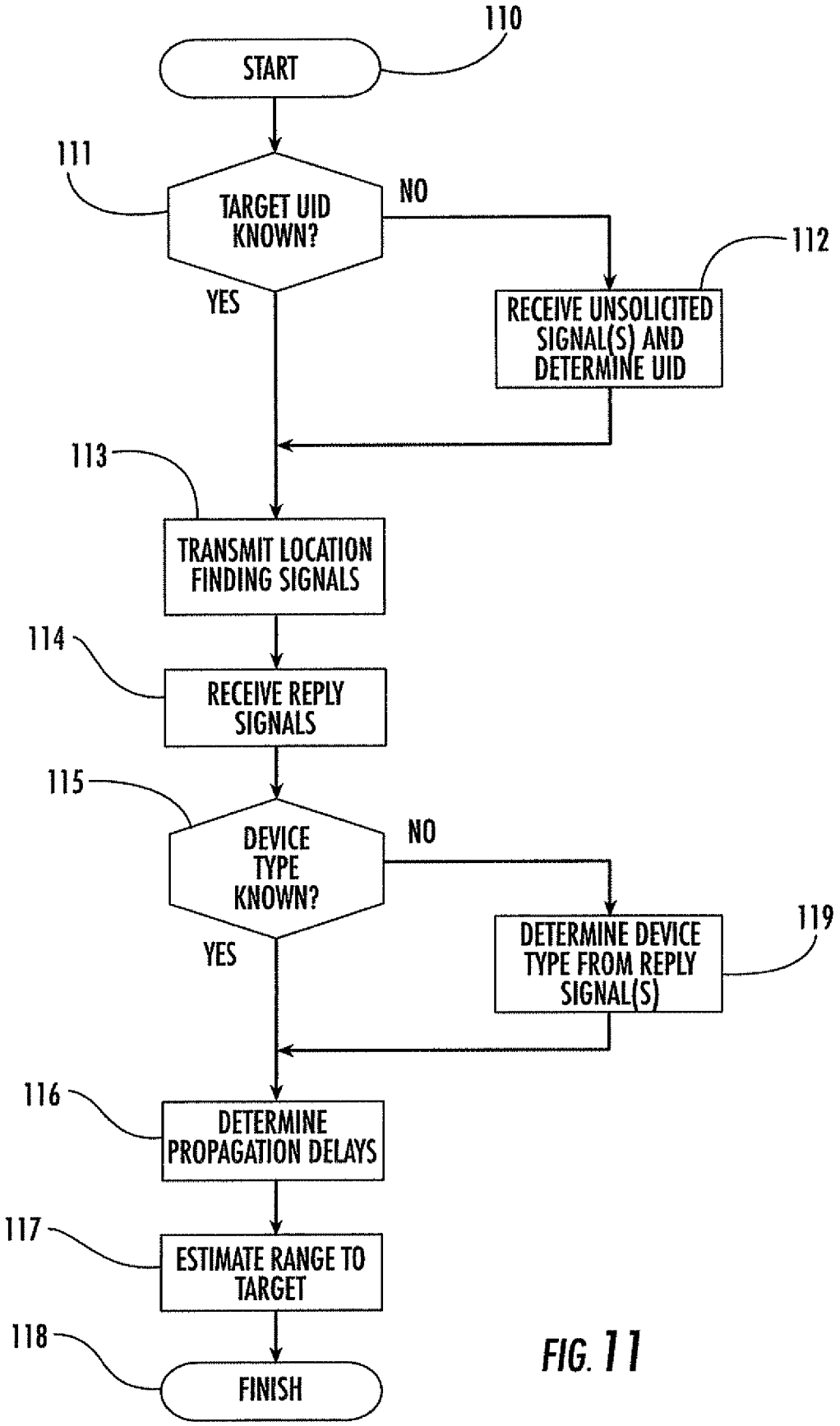

110
START
111
TARGET UID KNOWN?
NO
YES
112
RECEIVE UNSOLICITED SIGNAL(S) AND DETERMINE UID
113
TRANSMIT LOCATION FINDING SIGNALS
114
RECEIVE REPLY SIGNALS
115
DEVICE TYPE KNOWN?
NO
YES
119
DETERMINE DEVICE TYPE FROM REPLY SIGNAL(S)
116
DETERMINE PROPAGATION DELAYS
117
ESTIMATE RANGE TO TARGET
118
FINISH

FIG. 11

WIRELESS COMMUNICATIONS SYSTEM INCLUDING A WIRELESS DEVICE LOCATOR AND RELATED METHODS

FIELD OF THE INVENTION

The present application is a continuation of U.S. patent application serial No. 10/767,794 filed Jan. 29, 2004 now U.S. Pat. No. 7,110,779, the entire content of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

wireless location techniques are used in numerous applications. Perhaps the most basic of these applications is for locating lost articles. By way of example, published U.S. patent application Ser. No. 2003/0034887 to Crabtree et al. discloses a portable article locator system for locating lost articles such as glasses, keys, pets, television remotes, etc. More particularly, a wireless transceiver is attached to a person, animal, or other object. A handheld locator transmits a locator signal to the wireless transceiver which includes a unique address code of the transceiver. If the received code matches that stored by the wireless transceiver, it sends a return signal back to the locator device. The locator device uses the return signal to determine the distance and/or direction to the wireless transceiver from the user's location.

The locator device includes an antenna array which includes a plurality of omni-directional antennas. The locator unit determines the bearing to the wireless transceiver by switching between antennas in the antenna array and using Doppler processing to determine a direction of a wireless signal received from the transceiver. The distance to the wireless transmitter is also determined based upon the reception of the wireless signal at each of the antennas of the antenna array. Furthermore, in one embodiment, which is intended to avoid interference between two or more locators in a common area, a plurality of locator signals may be sent from a locator at a standard repetition rate. The locator's receiver then only listens for responses during predetermined windows following each transmission.

In contrast, in some applications it is desirable to determine the location of an unknown signal transmitter. U.S. Pat. No. 5,706,010 to Franke discloses such a system in which a transmitter locator receives a signal from the unknown signal transmitter and processes the signal to determine a bearing to the unknown signal transmitter. The transmitter locator then sends an interrogating signal to the unknown signal transmitter. Upon receiving the interrogating signal, the unknown signal transmitter heterodynes the interrogation signal with its own carrier signal to generate an intermodulation return signal. A processor of the transmitter locator measures the round-trip transit time from the transmission of the interrogation signal to the reception of the intermodulation return signal. A range to the unknown signal transmitter is then calculated based upon the round-trip transit time.

Still another application in which locating a wireless communications device is often necessary is in cellular telephone networks. That is, it may be necessary to locate particular cellular telephone users for law enforcement or emergency purposes, for example. U.S. Pat. No. 6,292,665 to Hildebrand et al., which is assigned to the present assignee, discloses a method for geolocating a cellular phone initiating a 911 call. A base station transceiver transmits a supervisory audio tone (SAT), which is automatically looped back by the calling cellular phone. Returned SAT signals are correlated with those transmitted to determine the range of the cellular phone. In addition, incoming signals from the cellular phone, such as the returned SAT signals, are received by a phased array antenna and subjected to angle of arrival processing to determine the direction of the cellular phone relative to the base station. The cellular phone is geolocated based upon the angle of arrival and the range information. A correction factor provided by the manufacturer of a given cellular telephone is used to account for the loopback path delay through the phone.

One additional area in which wireless device location can be important is in wireless networks, such as wireless local area networks (WLANs) or wide area networks (WANs), for example. A typical prior art approach to locating terminals within a WLAN includes locating a plurality of receivers at fixed locations within a building, for example, and then determining (i.e., triangulating) the position of a terminal based upon a signal received therefrom at each of the receivers.

Another prior art approach for wireless terminal location is to use a direction finding (DF) device which includes a directional antenna for receiving signals when pointed in the direction of a transmitting node. An example of a portable DF device for WLANs is the Yellowjacket 802.11a wi-fi analysis system from Berkeley Varitronics. This device uses a passive DF technique, i.e., it does not solicit any signals from a terminal but instead waits for the terminal to transmit signals before it can determine the direction of the transmission.

Despite the advantages of such prior art wireless communications device locators, additional wireless location features may be desirable in various applications.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a wireless communications device locator which provides enhanced location features and related methods.

This and other objects, features, and advantages in accordance with the present invention are provided by a wireless communications system which may include a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types. Further, each device type may have a known device latency associated therewith. The system may also include a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality of wireless communications devices. The target wireless communications device may transmit a respective reply signal for each of the location finding signals.

Additionally, the controller of the wireless device locator may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor. This may be done based upon the known device latency of the target wireless communications device. As such, the controller may estimate a range to the target wireless communications device based upon a plurality of determined propagation delays.

In other words, the wireless device locator advantageously provides active range finding. In other words, the

wireless device locator prompts the target wireless communications device to send reply signals using the location finding signals, rather than passively waiting until the target wireless communications device begins transmitting. This allows for quicker and more efficient device location.

Furthermore, by estimating the range based upon a plurality of propagation delays, the wireless device locator mitigates the effects of variations in the device latency time. That is, while the target wireless communication device has a known device latency, there will necessarily be some amount of variance from one transmission to the next. Using a plurality of propagation delays associated with different transmissions provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller may estimate the range based upon an average (e.g., mean, median, mode, etc.) of the propagation delays.

In addition, each wireless communications device may have a unique identifier (UID) associated therewith, and the controller may insert the UID for the target wireless communications device in each of the location finding signals. Furthermore, the target wireless communications device may generate respective reply signals based upon the UID in the location finding signals. That is, the target wireless communications device will act upon the location finding signals because these signals include its UID, whereas the other wireless communications device will not.

The target wireless communications device may generate unsolicited signals including the UID thereof. As such, the controller may cooperate with the transceiver to receive at least one unsolicited signal from the target device, and the controller may also determine the UID for the target device from the at least one unsolicited signal. Thus, if the UID of a target wireless communications device is not already known, the wireless device locator may passively "listen" for unsolicited signals therefrom (i.e., signals that the wireless communications device did not solicit) and determine the UID based thereon.

Additionally, the controller may also determine the device type of the target wireless communications device based upon the UID. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. Accordingly, the controller may determine the device type of the target wireless communications device based upon the MAC address in some applications.

In accordance with another advantageous aspect of the invention, the at least one antenna may be a plurality of antennas, and the controller may cooperate with the plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals. More particularly, the bearing may be a three-dimensional bearing, which may be particularly useful for locating wireless communications devices within a multi-story building, for example. In particular, the antenna(s) may be one or more directional antennas, for example. Further, the wireless device locator may further include a portable housing carrying the at least one antenna, the transceiver, and the controller.

The wireless device locator may be used with numerous type of wireless communications device. For example, the wireless communications devices may be wireless local area network (WLAN) devices, mobile ad-hoc network (MANET) devices, and cellular communications devices.

A method aspect of the invention is for locating a target wireless communications device from among a plurality of wireless communications devices, such as those discussed briefly above. The method may include transmitting a plurality of location finding signals to the target wireless communications device, and receiving a respective reply signal for each of the location finding signals therefrom. The method may further include determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device. As such, a range to the target wireless communications device may be estimated based upon a plurality of determined propagation delays.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is schematic block diagram of a wireless communications system in accordance with the present invention including a wireless local area network (WLAN) and wireless device locator for locating WLAN devices thereof.

FIG. **2** is a schematic block diagram generally illustrating the components of the wireless device locator of FIG. **1**.

FIG. **3** is a graph illustrating the signal propagation delay and device latency components used by the controller of FIG. **2** to estimate range.

FIG. **4** is a schematic block diagram illustrating an embodiment of the wireless device locator of FIG. **2** for a WLAN implementation.

FIG. **5** is a schematic block diagram illustrating in greater detail an embodiment of the transceiver of the wireless device locator of FIG. **4**.

FIGS. **6** and **7** are histograms illustrating range estimation test results performed using the wireless device locator of FIG. **4**.

FIG. **8** is a graph illustrating bearing determination in accordance with the present invention.

FIGS. **9** and **10** are schematic block diagrams illustrating alternate embodiments of the wireless communications system of FIG. **1** including a mobile ad-hoc network (MANET) and a cellular network, respectively.

FIG. **11** is a flow diagram illustrating a wireless device location method in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime and multiple prime notation are used to indicate similar elements in different embodiments.

Referring initially to FIGS. **1** and **2**, a wireless communications system **30** illustratively includes a wireless local area network (WLAN) **31** and a wireless location device **32**. The WLAN **31** illustratively includes an access point **33** (e.g., a server) and a plurality of WLAN devices or terminals which communicate therewith wirelessly, such as the laptop computers **34**, **35**, and the desktop computer **36**. Various WLAN protocols may be used in accordance with the present invention for such wireless communications (e.g., IEEE 802.11, Bluetooth, etc.), as will be appreciated by those of skill in the art. Moreover, it will also be appreciated that additional access points and/or other numbers of wire-

less communications devices may be used, even though only a few number thereof are shown for clarity of illustration. Further, numerous other types of WLAN enabled wireless communications devices (e.g., personal data assistants, etc.) may also be used, as will be further appreciated by those skilled in the art.

Each wireless communications device **34-36** in the WLAN **31** has a device type associated therewith from among a plurality of different device types. More particularly, the device type may signify the particular manufacturer and/or model of a given WLAN card or chip set used therein. In some embodiments, it may also signify the standard the device complies with (e.g., IEEE 802.11).

The device type is important in that different device types will have known device latencies associated therewith. For example, different WLAN cards or chip sets will have a certain latency associated with the time they take to process a received signal and generate an acknowledgement reply thereto. These delay times may be fairly consistent across different models from a same manufacturer, or they may vary significantly. Additionally, WLAN protocols such as IEEE 802.11 have a specified interframe spacing associated therewith, as will be appreciated by those skilled in the art. Thus, in circumstances where the interframe spacing requirements are closely adhered to, the latency of a given WLAN card or chip set will be substantially equal to the interframe spacing.

The wireless device locator **32** illustratively includes an antenna **39** and a transceiver **41** connected thereto, as well as a controller **42** connected to the transceiver. These components may conveniently be carried by a portable housing **43** in some embodiments, although they could be implemented in a more stationary embodiment, if desired. In the illustrated example, the antenna **39** is a directional antenna, although omni-directional antennas may also be used, as will be appreciated by those skilled in the art. It will also be appreciated that various antenna/transceiver combinations may be used. As will be discussed further below, more than one antenna may be used in certain embodiments to provide bearing determination capabilities, and separate transceivers may optionally be used for respective antennas, if desired.

Operation of the wireless device locator **32** will now be described with reference to FIG. **3**. The controller **42** cooperates with the transceiver **41** for transmitting a plurality of location finding signals to a target wireless communications device to be located from among the plurality of wireless communications devices. In the present example, the laptop **34** is the target device.

As will be appreciated by those skilled in the art, each WLAN device **34-36** in the network **31** will have a unique identifier (UID) associated therewith which is used in signals transmitted between the respective devices and the access point **33**. The UID distinguishes the devices **34-36** from one another so that each device only acts upon or responds to signals intended for it, and so the access point **33** knows which device it is receiving signals from.

Depending upon a given implementation, the wireless locator device **32** may or may not know the UID of the target device **34** before hand. For example, in some embodiments the wireless device locator **32** could download the UID from the access point **33** (either wirelessly or over a wired network connection, for example). This may be the case when trying to locate a node in a LAN where the node is already registered with the network. However, if the UID is not known, the wireless device locator **32** may passively listen to the target device **34** for unsolicited signals being transmitted therefrom. This feature may be advantageous for law enforcement applications, or for locating an interfering node that is not registered with a particular network but causes interference therewith, for example. By "unsolicited" signals it is meant that these signals are not solicited by the wireless device locator **32** itself, although such signals may have been solicited from another source (e.g., the access point **33**).

The controller **42** cooperates with the transceiver **41** to receive one or more of the unsolicited signals, and the controller determines the UID for the target device **34** therefrom. Of course, the method by which the controller **42** determines the UID from the unsolicited signal will depend upon the given implementation, and whether or to what degree such signals are encrypted.

Additionally, the controller **42** may also determine the device type of the target wireless communications device **34** based upon the UID thereof. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. The MAC addresses may be specific to a particular type of device manufacturer, or indicate a particular operational protocol with which the device is operating, as will be appreciated by those skilled in the art. Accordingly, the controller may determine the device type of the target wireless communications device **34** based upon the MAC address thereof in some applications.

As such, to locate the target device **34**, the controller inserts the UID therefor in each of the location finding signals. By way of example, the location finding signal may include the UID of the target device **34** in a header packet and a valid but empty data packet. This will force the target device **34** to generate a reply signal acknowledging receipt of the location finding signal (i.e., an ACK signal). Of course, various other location finding signals could be used to cause the target terminal **34** to generate an ACK signal, as will be appreciated by those skilled in the art. The controller **42** cooperates with the transceiver **41** for receiving the reply signals from the target device **34** via the antenna **39**. The location finding signals and reply signals may be radio frequency (RF), microwave, optical, or other suitable types of signals, as will be appreciated by those skilled in the art.

The controller **42** determines the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor, and it uses this propagation delay to estimate a range to the target device **34**. However, the propagation delay has to first be determined based upon the total round trip time from the sending of the location finding signal to the reception of the respective reply signal.

The total round trip time will include several components. Referring more particularly to FIG. **3**, the first component is the time associated with transmitting a location finding signal **45**, which is illustrated with an arrow. That is, this is the time from the beginning of the location finding signal transmission (time t_0) to end thereof (time t_1). Two time axes are shown in FIG. **3**. The top or upper axis represents events that occur at the target device **34**, while the bottom or lower axis represents events that occur at the wireless device locator **32**.

The second component of the round trip time is the propagation delay or time t_{PD1} it takes for the location finding signal **45** to travel from the wireless device locator **32** to the target device **34** (i.e., from time t_1 to t_2). The third component of the round trip time is the device latency t_{DL} of the target device **34** (i.e., form time t_2 to t_3). This is the time it takes the target device **34** to receive, process, and transmit a reply signal **46** responsive to the location finding signal **45**.

The final components of the round trip time are propagation delay t_{PD2} of the reply signal **46** (i.e., from time t_3 to t_4), and the reception time thereof by the wireless device locator **32** (i.e., from time t_4 to t_5).

The controller **42** will know the times associated with the transmission of the location finding signal **45** (i.e., from time t_0 to t_1), as well as the time associated with the reception of the reply signal **46** (i.e., from time t_4 to t_5) for each round trip, since these can be readily measured by the controller. The quantities that the controller **42** will not know are the propagation delays t_{PD1}, t_{PD2} and the actual device latency t_{DL}.

Yet, as noted above, the controller **42** will have access to the known device latency (i.e., a mean latency) for the given device type of the target device **34**, which provides a close approximation of the actual device latency t_{DL}. The known device latency could be a measured value based upon collected data, it could be provided by manufacturers, or it could be based upon a value set in a communications standard, as discussed above, for example.

As will be appreciated by those skilled in the art, the actual device latency will likely vary somewhat from one transmission to the next for any wireless communications device, potentially by as little as a few nanoseconds to a few microseconds, depending upon device configurations, processing loads, etc. Accordingly, a close approximation of the total propagation delay (i.e., time t_{PD1}+time t_{PD2}) may therefore be obtained by substituting the known device latency for the actual device latency t_{DL}, and subtracting this value from the time between times t_1 and t_4. Dividing the total propagation delay by two (since both propagation delays may be considered equal or substantially equal for a stationary or relatively slow moving target device **34**) and multiplying this by the speed of light gives the estimated distance to the target device **39**, based upon the single propagation delay associated with the signal pair **45**, **46**.

Yet, as noted above, device latencies tend to vary from one transmission to the next. Since the location finding signals and reply signals are traveling at the speed of light, such variances can make a significant difference in the estimated distances. More particularly, light travels approximately 1000 ft. in one microsecond. Thus, if the device latency varies by one microsecond from one transmission to the next, the estimated distance to the target device **34** would similarly vary by 1000 ft. or so, which likely will be an unacceptable accuracy for many applications.

In accordance with the present invention, the controller **42** advantageously estimates the range to the target device **34** not solely based upon a single measured propagation delay, but rather upon a plurality thereof. More particularly, by estimating the range based upon a plurality of propagation delays, the wireless device locator **32** mitigates the effects of the variations in the actual device latency time. This provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller **42** may estimate the range based upon an average of the propagation delays, though other suitable statistical functions may also be used (e.g., mean, median, mode, etc.). Of course, it should be noted that the average may be taken on the entire round trip delay instead of first subtracting out the known device latency as described above. That is, the same result may be obtained by first taking the average and then subtracting out the known device latency, as will be appreciated by those skilled in the art.

An exemplary embodiment of the present invention is now described with reference to FIGS. **4** and **5**. The wireless device locator **32'** may use a personal data assistant (PDA) as the controller **42'**, although a personal computer (PC) or other suitable computing device may also be used. More particularly, the PDA **42'** illustratively includes a graphical user interface (GU1) **50'**, and a received signal strength indication (RSSI) processing module **51'** for cooperating with the transceiver **41'** to perform above described range estimation processing operations. More particularly, the RSSI module **51'** may be implemented as a software module which is run on the PDA **42'**, as will be appreciated by those skilled in the art, and which cooperates with the GUI to provide range estimates to a user.

The PDA **50'** also illustratively includes a battery **52'**, which may conveniently be used for powering the various transceiver **41'** components, as shown. Of course, it will be appreciated that separate batteries may be used, or one or more components of the wireless device locator **32'** may be powered by an external (e.g., AC) source. The transceiver **41'** operates in accordance with the IEEE 802.11b standard and includes a MAC-less 802.11b radio **58'** and a field-programmable gate array (FPGA) **53'** connected thereto. The FPGA **53'** illustratively includes a packet building module **54'**, a radio configuration module **55'**, a receiver filtering module **56'**, and a simple MAC processing module **57'** for processing the location finding signals and reply signals and communicating with the radio **53'**, in accordance with the 802.11b standard, as will be appreciated by those skilled in the art.

More specifically, the MAC-less radio **58'** may be a GINA model EF module from GRE America, Inc., and the FPGA **53'** may be a module EPXA10 from Altera Corp. The hardware components of the FPGA **53"** illustratively include an ARM922T processor **60"**, block RAM **61"** therefor, a serial/universal serial bus (USB) interface **62"**, and a programmable logic section **63"**. Additional circuitry including an oscillator **64"**, power management circuitry (i.e., regulators, microprocessor supervisor, etc.) **65"**, and a programmable read-only memory (PROM)/boot flash memory **66"** are connected thereto as shown, as will be appreciated by those skilled in the art.

Referring now to FIGS. **6-7**, a test was conducted in accordance with the present invention in which approximately 1500 location finding signals were transmitted to a stationary wireless IEEE 802.11 device. The time it took to receive the reply signal was measured by ticks of an internal clock of the controller **42**, where each tick represents 7.567 ns. From FIG. **6** it may be seen that the reply signals from the target device were returned within between about 20,960 and 21,045 clock ticks, where the transmission of the respective location signals each began at 0 clock ticks. Moreover, if this range is divided into equal sections or bins, the frequency (i.e., number) of round trip times that fell within each of the bins is shown in FIG. **7**.

Plotting various statistical functions of the measured clock tick samples (such as the mean and the mode) versus the known distance to the target device allowed statistical curve-fitting to take place, as shown in FIG. **6**. It was determined from the test results that taking the mean of the samples provided the most accurate range estimation. More particularly, the ranges to several 802.11b target devices at varying distances were estimated using this approach, and the worst case error for the estimated range was never more than 20 ft. Preferably, the location finding signals are transmitted over a relatively short interval (a few seconds or less) so that if the target device is moving the accuracy of the results will not be significantly diminished. Of course, various numbers of location finding signals and transmission

intervals may be used depending upon the particular implementation, as will be appreciated by those skilled in the art.

In accordance with another advantageous aspect of the invention, multiple antennas **39**a", **39**b" (FIG. **5**) may be used to provide target bearing in addition to the estimated range. Referring more particularly to FIG. **8**, bearing determination in the case where the antennas **39***a*", **39***b*" are directional antennas will now be described. The antennas **39***a*", **39***b*" have respective reception patterns **70***a*, **70***b*, which may be orthogonal to one another (i.e., the former is directed along the x-axis, while the latter is directed along the y-axis).

The target device is at a point P, which is within the reception patterns **70***a*, **70***b*. Each of the antenna gain patterns **70***a* and **70***b* can be measured and known to the locator, and represented by gain functions G**1**(θ) and G**2**(θ) where e represents the angle of deviation from a particular reference direction.

As such, to determine the line of bearing to the target device, the received signal strength is measured from each of the antennas **70***a*, **70***b*, respectively. Based upon this information, the controller **42'** may then find the angle θ_t using the relationship $G1(\theta_t)-G2(\theta_t)=P1-P2$, where P**1** and P**2** is the received signal power off antenna **1** and antenna **2**, respectively. In other words, the difference in the signal strength received between the two antennas (P**1**-P**2**) should equal the difference in the antenna gain of the two antennas at the angle of the line of bearing $(G1(\theta_t)-G2(\theta_t))$ Thus, the target line of bearing to the target device is at θ_t. It should be noted that it is possible that more than one angle θ may satisfy the relationship $G1(\theta_t)-G2(\theta_t)=P1-P2$. These multiple angles represent a line of bearing ambiguity that can easily be resolved by making multiple measurements, as can be appreciated by those skilled in the art.

As noted above, more than one transceiver **41'** may be used in certain embodiments, which would allow signal strength measurements to be taken based upon a same reply signal from the target device. However, if only a single transceiver **41'** is used, the controller **42'** may alternate which antenna **70***a*, **70***b* is receiving and measure the received signal strength of successive signals, for example. Moreover, the bearing may be determined in three dimensions, if desired, which may be particularly useful for locating wireless communications devices within a multistory building, for example, as will be appreciated by those skilled in the art.

While the present invention has been described above with reference to a WLAN wireless device locator **32'**, it will be appreciated by those skilled in the art that it may also be used in other wireless communications systems with other types of wireless communications devices. Referring more particularly to FIG. **9**, a mobile ad-hoc network (MANET) system **90** illustratively includes a wireless device locator **92** including an antenna **99**, such as those described above, and a MANET **91**. More particularly, the MANET includes MANET nodes or devices **93-96**, of which the node **94** is the target node in the illustrated example. Here, the wireless device locator **92** performs range and/or bearing estimation in the same manner described above, except that it will operate in accordance with the appropriate MANET protocol used within the system **90**, as will be appreciated by those skilled in the art.

Another embodiment is illustrated in FIG. **10**, in which a wireless device locator **102** having an antenna **109** is used within a cellular communications system **100** for locating cellular devices (e.g., cellular telephones) **104-106** in cellular network **101**. The cellular devices **104-106** place and receive calls via a cellar tower **103**, as will be appreciated by those skilled in the art. In the illustrated example, the target device is the cell phone **104**. Here again, the wireless device locator **102** will communicate using the appropriate operating protocol being used in the cellular network **101** (e.g., code-division multiple access (CDMA), short message service (SMS), etc.), as will be appreciated by those skilled in the art.

Turning now additionally to FIG. **11**, a method aspect of the invention is for locating a target wireless communications **34** device from among a plurality of wireless communications devices **34-36**. Beginning at Block **110**, if the UID for the target device **34** is unknown, the controller **42** may determine the UID from unsolicited signals transmitted by the target device, for example, as described above (Block **112**). Of course, in some embodiments, the controller **42** may download the signals from a network access point **33**, etc., as also described above.

Once the UID for the target wireless communication device **34** is known, location finding signals are transmitted to the target wireless communications device, at Block **113**, and respective reply signals for each of the location finding signals are received therefrom, at Block **114**. If the device type (and, thus, the known device latency) are known, at Block **115**, then the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor is determined based upon the known device latency of the target wireless communications device **34**, at Block **116**. As such, a range to the target wireless communications device **34** is estimated based upon a plurality of determined propagation delays (Block **117**), as previously discussed above, thus concluding the illustrated method (Block **118**).

Of course, if the device type is unknown, the controller **42** may determine the device type from the reply signal (Block **119**), as discussed above, or by other suitable methods which will be appreciated by those skilled in the art. It should be noted that while this step is shown as occurring after the receipt of the reply signals in the illustrated example, the device type determination may be performed prior thereto, such as while determining the UID, for example.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A wireless communications system comprising:

a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types, and each device type having a known device latency associated therewith; and

a wireless device locator comprising

at least one antenna and a transceiver connected thereto, and

a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among said plurality of wireless communications devices;

said target wireless communications device transmitting a respective reply signal for each of said location finding signals;

said controller of said wireless device locator also for

cooperating with said transceiver for receiving the reply signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target wireless communications device, and

estimating a range to said target wireless communications device based upon a plurality of determined propagation delays.

2. The wireless communications system of claim **1** wherein said controller estimates the range based upon an average of the propagation delays.

3. The wireless communications system of claim **1** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target wireless communications device based upon at least one of the received reply signals.

4. The wireless communications system of claim **3** wherein the bearing is a three-dimensional bearing.

5. The wireless communications system of claim **1** wherein said at least one antenna comprises at least one directional antenna.

6. The wireless communications system of claim **1** wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller.

7. The wireless communications system of claim **1** wherein said wireless communications devices comprise wireless local area network (WLAN) devices.

8. The wireless communications system of claim **1** wherein said wireless communications devices comprise mobile ad-hoc network (MANET) devices.

9. The wireless communications system of claim **1** wherein said wireless communications devices comprise cellular communications devices.

10. A wireless communications system comprising:

a plurality of wireless local area network (WLAN) devices each having a device type associated therewith from among a plurality of different device types, and each device type having a known device latency associated therewith; and

a wireless device locator comprising

at least one antenna and a transceiver connected thereto, and

a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target WLAN device from among said plurality of WLAN devices;

said target WLAN device transmitting a respective reply signal for each of said location finding signals;

said controller of said wireless device locator also for

cooperating with said transceiver for receiving the reply signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target WLAN device, and

estimating a range to said target WLAN device based upon an average of a plurality of determined propagation delays.

11. The wireless communications system of claim **10** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target WLAN device based upon at least one of the received reply signals.

12. A wireless device locator for locating a target wireless communications device comprising:

at least one antenna and a transceiver connected thereto; and

a controller for

cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device and receiving a respective reply signal therefrom for each of said location finding signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device, and

estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

13. The wireless device locator of claim **12** wherein said controller estimates the range based upon an average of the propagation delays.

14. The wireless device locator of claim **12** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals.

15. The wireless device locator of claim **12** wherein said at least one antenna comprises at least one directional antenna.

16. The wireless device locator of claim **12** wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller.

17. The wireless device locator of claim **12** wherein the target wireless communications device comprises a wireless local area network (WLAN) device.

18. The wireless device locator of claim **12** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

19. The wireless device locator of claim **12** wherein the target wireless communications device comprises a cellular communications device.

20. A method for locating a target wireless communications device from among a plurality of wireless communications devices, each wireless communications device having a device type associated therewith from among a plurality of different device types, and each device type having a known device latency associated therewith, the method comprising:

using a controller cooperating with a transceiver for transmitting a plurality of location finding signals to the target wireless communications device, and receiving a respective reply signal for each of the location finding signals therefrom;

using the controller for determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device; and

further using the controller for estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

21. The method of claim **20** wherein the controller estimates the range based upon an average of the propagation delays.

22. The method of claim **20** further comprising determining a bearing to the target wireless communications device based upon at least one of the received reply signals.

23. The method of claim **20** wherein the target wireless communications device comprises a wireless local area network (WLAN) device.

24. The method of claim **20** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

25. The method of claim **20** wherein the target wireless communications device comprises a cellular communications device.

* * * * *

Exhibit 4

US007765399B2

(12) **United States Patent**
O'Brien

(10) **Patent No.: US 7,765,399 B2**
(45) **Date of Patent: *Jul. 27, 2010**

(54) **COMPUTER ARCHITECTURE FOR A HANDHELD ELECTRONIC DEVICE**

(75) Inventor: **Terence W. O'Brien**, Webster, NY (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1192 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/359,224**

(22) Filed: **Feb. 22, 2006**

(65) **Prior Publication Data**

US 2007/0199046 A1 Aug. 23, 2007

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/164**; 726/16

(58) **Field of Classification Search** 713/189, 713/164, 176, 181; 726/1, 36, 26; 380/49, 380/4, 9, 25, 30, 40–60; 455/410
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,092,202 A * 7/2000 Veil et al. 726/27
7,028,149 B2 * 4/2006 Grawrock et al. 711/156
7,047,405 B2 * 5/2006 Mauro 713/166
2006/0105740 A1 * 5/2006 Puranik 455/410

FOREIGN PATENT DOCUMENTS

GB 2336005 A * 10/1999

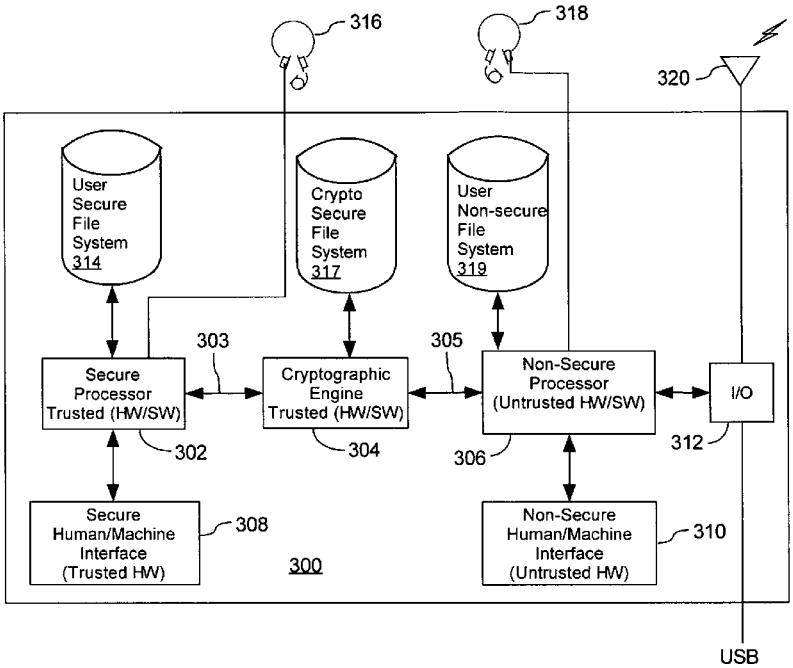
* cited by examiner

Primary Examiner—Pramila Parthasarathy
(74) *Attorney, Agent, or Firm*—Fox Rothschild, LLP; Robert J. Sacco

(57) **ABSTRACT**

Mobile PDA computer system (**300**) includes a non-secure processor (**306**), comprising an untrusted microprocessor and an untrusted operating system executing on the untrusted microprocessor. The system also includes a secure processor (**302**), comprising a trusted microprocessor and a trusted operating system executing on the trusted microprocessor. A cryptographic engine (**304**) is provided for encrypting and decrypting data. A first data communication link (**303**) communicates data between the secure processor and the cryptographic engine. A second data communication link (**305**) communicates data between the non-secure processor and the cryptographic engine. In this way, the cryptographic engine forms a bridge between the secure user processor and the non-secure user processor.

19 Claims, 4 Drawing Sheets



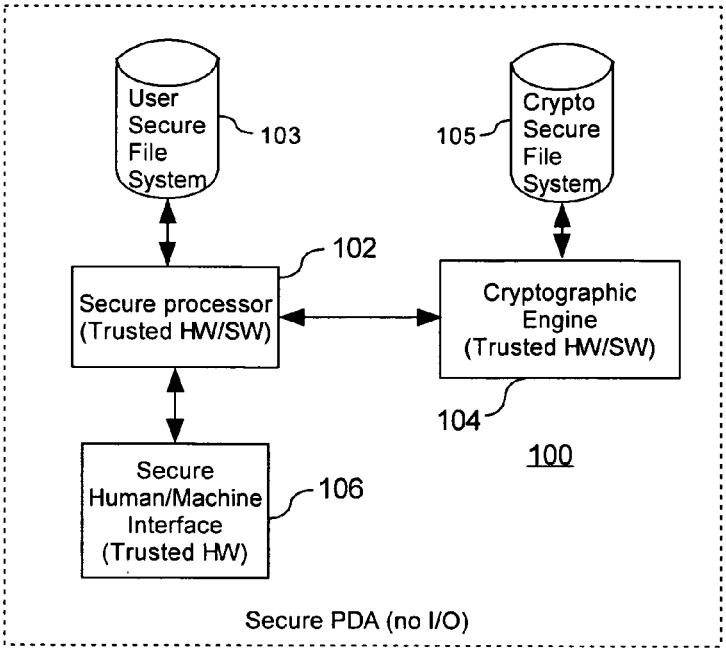


Fig. 1
(Prior Art)

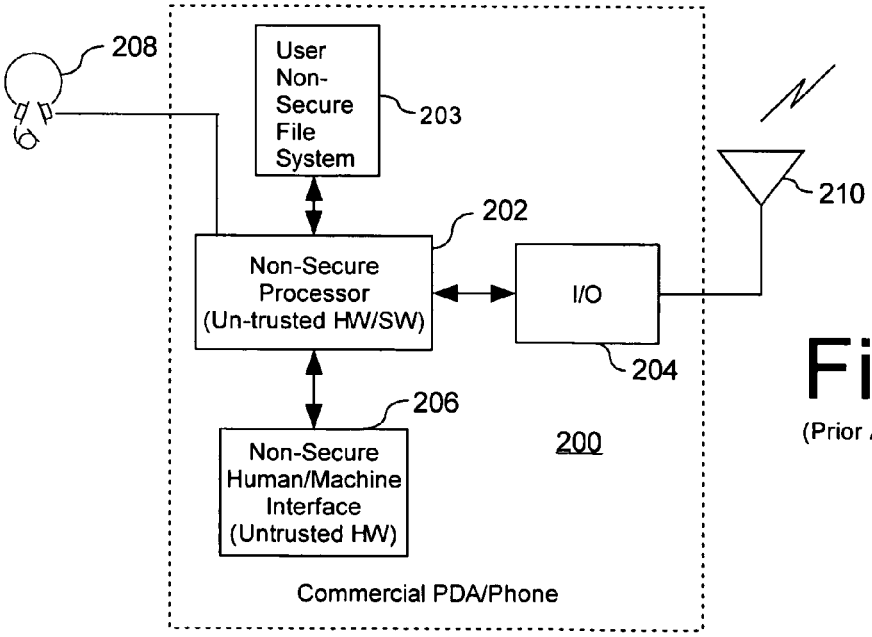


Fig. 2
(Prior Art)

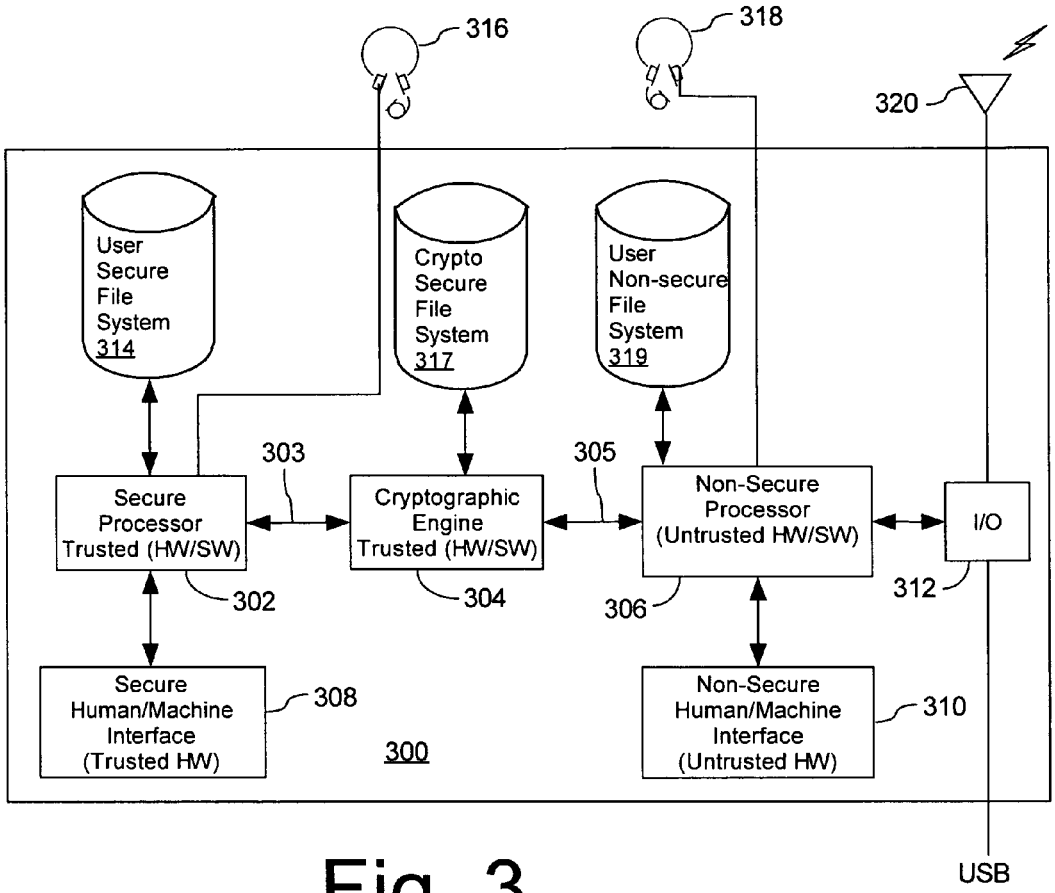

316
318
320
User Secure File System 314
Crypto Secure File System 317
User Non-secure File System 319
303
305
Secure Processor Trusted (HW/SW)
Cryptographic Engine Trusted (HW/SW)
Non-Secure Processor (Untrusted HW/SW)
I/O
302
304
306
312
Secure Human/Machine Interface (Trusted HW)
308
300
Non-Secure Human/Machine Interface (Untrusted HW)
310
USB

Fig. 3

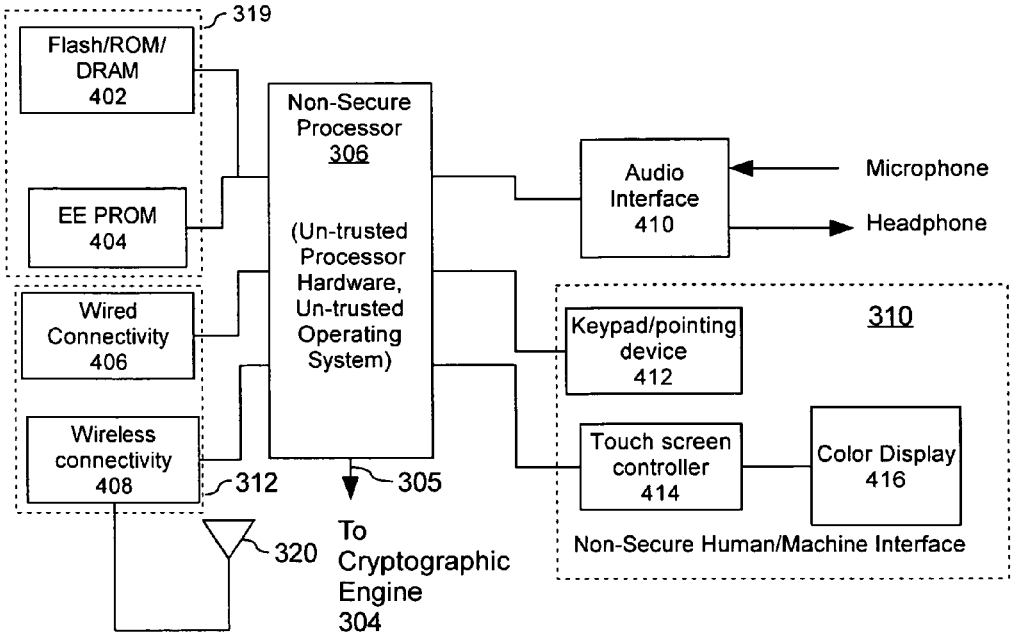

319
Flash/ROM/ DRAM 402
EE PROM 404
Wired Connectivity 406
Wireless connectivity 408
312
320
Non-Secure Processor 306
(Un-trusted Processor Hardware, Un-trusted Operating System)
305
To Cryptographic Engine 304
Audio Interface 410
Microphone
Headphone
310
Keypad/pointing device 412
Touch screen controller 414
Color Display 416
Non-Secure Human/Machine Interface

Fig. 4

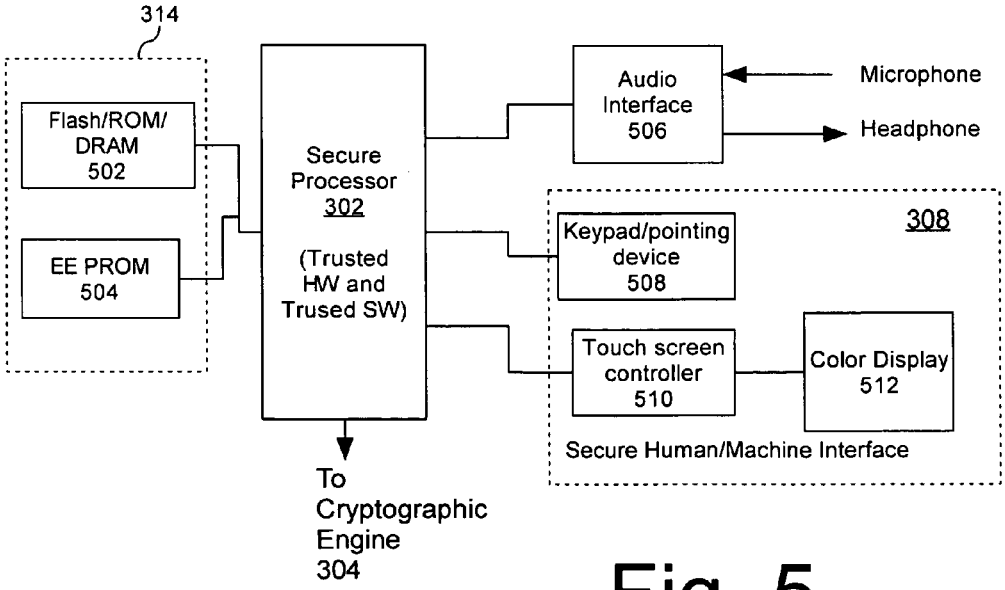

314
Flash/ROM/ DRAM 502
EE PROM 504
Secure Processor 302
(Trusted HW and Trused SW)
To Cryptographic Engine 304
Audio Interface 506
Microphone
Headphone
308
Keypad/pointing device 508
Touch screen controller 510
Color Display 512
Secure Human/Machine Interface

Fig. 5

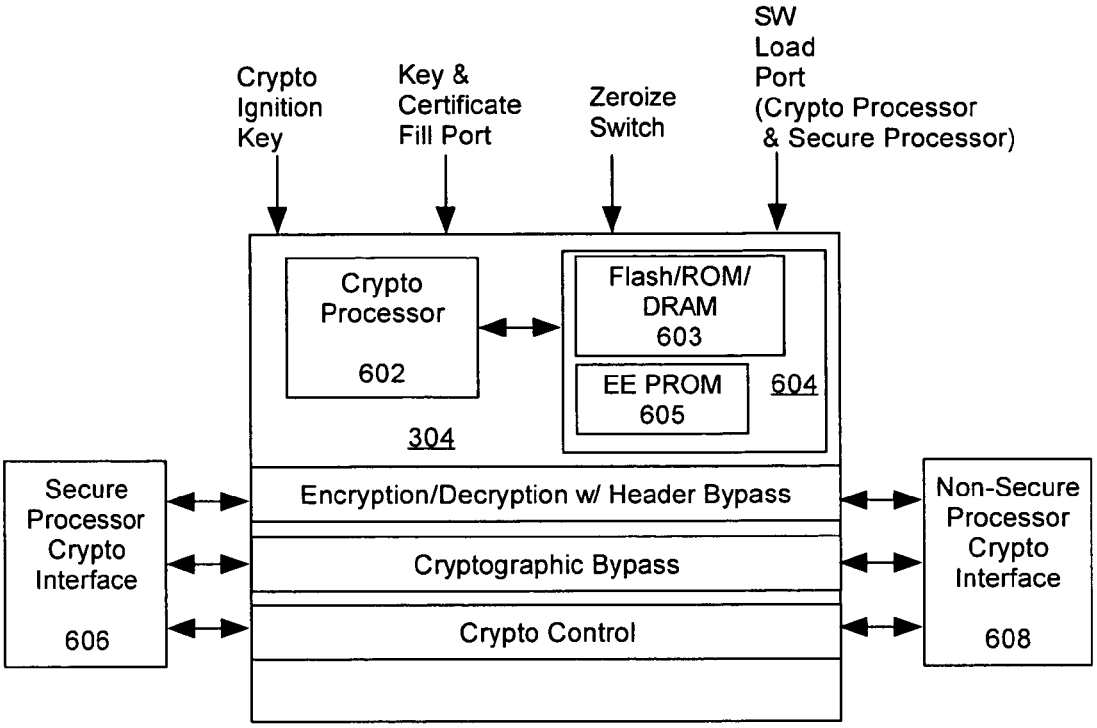

Crypto Ignition Key
Key & Certificate Fill Port
Zeroize Switch
SW Load Port (Crypto Processor & Secure Processor)
Crypto Processor 602
Flash/ROM/ DRAM 603
EE PROM 605
604
304
Secure Processor Crypto Interface 606
Encryption/Decryption w/ Header Bypass
Cryptographic Bypass
Crypto Control
Non-Secure Processor Crypto Interface 608

Fig. 6

COMPUTER ARCHITECTURE FOR A HANDHELD ELECTRONIC DEVICE

BACKGROUND OF THE INVENTION

1. Statement of the Technical Field

The inventive arrangements relate to personal electronic devices, and more particularly to personal digital assistant devices for storing, processing and communicating classified as well as unclassified data.

2. Description of the Related Art

Mobile computers, which are sometimes called personal digital assistants or PDAs, have the ability to store, process and communicate data. PDAs generally fall into one of several categories which can include handheld PCs, palm size PCs, smart phones, and handheld instruments. PDAs typically include some kind of microprocessor with a commercially available operating system such as Linux, Palm OS, or Widows CE (Pocket PC). Many PDAs also have built in LCD displays, touch sensitive screens, and keypads for the human/machine interface. Some PDAs also include wireless networking capabilities. For example, many such devices can communicate with other devices using well known wireless networking standards such as the IEEE 802.11 family of standards. The foregoing capabilities make these compact devices highly useful for a various business and personal applications.

Currently, there exist a wide variety of PDA devices with conventional operating systems and architectures. These commercially available PDAs with commercial-off-the-shelf (COTS) operating systems and COTS application programs generally satisfy the processing and communications requirements of most users. For example, they include applications for word processing, data storage, spreadsheets, email, internet browsing, time management, contact management, network communications, and voice communications. These applications generally function quite well and have interfaces that are familiar to many users. The familiarity of these applications to users, and the relatively low cost of COTS software are considered advantageous for a variety of reasons.

Some commercially available PDA devices and/or software applications incorporate various security measures in an effort to protect data which is stored, processed or communicated using the device. For example, encryption technology and password protection features are known in the art. Still, this level of security can be inadequate for managing information that is of a Confidential, Secret, or Top Secret nature, particularly when such information relates to matters of national security. For example, COTS operating systems and applications may not be sufficiently trustworthy for handling this type of information. Such programs can be susceptible to being compromised by various means including hacker attacks, viruses, worms, Trojan horses, and a wide variety of other means that are known to those skilled in the art.

Finally, notwithstanding the security limitations of COTS operating systems and applications, the basic architecture and interface systems of many commercial PDA devices may leave these devices vulnerable to intrusion. For example, COTS devices do not employ trusted microprocessors, do not employ physical separation of classified and unclassified data processing, nor do they employ physical tamper detection and subsequent memory zeroization. They may also lack the capability of wireless communications for classified data. Consequently, transport, processing or communication of classified data using a commercial PDA is not generally permitted.

In order to address some of the foregoing problems, personal electronic devices have been developed that are specifically designed to allow for transport of classified data, for example encryption keys. However, these devices are not generally designed to accommodate data processing or wireless communications of classified information. Secure PDA devices are also known in the art. These devices utilize a trusted operating system, trusted microprocessors, and a trusted human/machine interface. However, they generally do not include wireless communications capabilities.

Trusted operating systems and applications are generally designed to more rigorously address the problem of computer security. Trusted operating systems undergo evaluation of their overall design, verification of the integrity and reliability of their source code, and systematic, independent penetration evaluation. In contrast, non-trusted COTS operating systems are generally not designed to an equally high level with regard to security precautions.

SUMMARY OF THE INVENTION

The invention concerns a mobile PDA computer system. The mobile PDA computer system consists of a non-secure user processor, a secure user processor, and a cryptographic engine. The non-secure processor is comprised of non-trusted COTS microprocessor hardware (HW), a non-trusted COTS operating system, and non-trusted COTS application software. The secure processor is comprised of trusted microprocessor HW, a trusted operating system and trusted application software. The cryptographic engine is comprised of trusted hardware and trusted software. In addition to providing encryption and decryption services, the cryptographic engine provides a first data communication link that communicates data between the secure processor and the cryptographic engine and a second data communication link that communicates data between the non-secure processor and the cryptographic engine. In this way, the cryptographic engine forms a bridge between the secure processing side of the PDA and the non-secure processing side of the PDA.

According to one aspect of the invention, the non-secure processor can have a wired communication transceiver and/or a wireless communications transceiver. These communication transceivers can be used to communicate unclassified data and voice transmissions. In addition these transceivers can be used to communicate encrypted classified data. The secure processor can communicate encrypted classified data files from the secure processor's file system to the non-secure processor. The encrypted files can then be communicated using the wired or wireless transceiver circuitry associated with the non-secure processor. Similarly, classified real time voice communications originating on the secure processing side of the device can be encrypted and communicated to the non-secure processor. The non-secure processor can utilize the wired or wireless transceiver to communicate such encrypted voice information.

The invention can also concern a method for managing classified and unclassified on a mobile PDA computer system. The method can include processing classified data exclusively using a secure processor. The method can also include processing unclassified data exclusively using a non-secure processor. Classified data for encryption and classified decrypted data can be communicated between the secure processor via the cryptographic engine using a first data communication link. Further classified data from the secure processor via the cryptographic engine can be communicated to the non-secure processor exclusively in an encrypted form.

Such communications can be performed using a second data communication link between the cryptographic engine and the non-secure processor.

The method can include communicating classified data to and from the secure processor exclusively using a secure human/machine interface. Further, the method can include controlling the secure processor exclusively using the secure human/machine interface. Classified information can be provided to the user from the secure processor exclusively using the secure human/machine interface.

The non-secure processor can be controlled exclusively using a non-secure human/machine interface. Further, unclassified information can be provided to the user by the non-secure processor exclusively using the non-secure human/machine interface. A wireless communications transceiver can be used for communicating wireless unclassified data from the non-secure processor. The method can further include communicating encrypted classified data provided from the secure processor using the wireless communications transceiver. According to one aspect of the invention, the wireless communications transceiver can be selected from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver. According to yet another aspect, the method can include communicating classified audio information to and from the secure processor with a first audio interface, and communicating audio information to and from the non-secure processor with a second audio interface distinct from the first audio interface.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is block diagram that is useful for understanding an architecture of a secure PDA

FIG. **2** is a block diagram that is useful for understanding an architecture of a non-secure commercial PDA/Phone.

FIG. **3** is a block diagram that is useful for understanding an architecture of a PDA that can be used for classified and unclassified data.

FIG. **4** is a more detailed block diagram showing the non-secure processor portion of the PDA architecture in FIG. **3**.

FIG. **5** is a more detailed block diagram showing the secure processor portion of the PDA architecture in FIG. **3**.

FIG. **6** is a more detailed block diagram of the cryptographic engine in FIG. **3**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention concerns a computer architecture for a mobile PDA computer system. FIG. **1** shows a simplified block diagram of a secure PDA of the prior art that includes trusted hardware and trusted software (operating system and application software). As used herein, the term "trusted" is used with reference to computer hardware, operating systems, and/or software applications that have been designed to ensure secure storage, processing and communication of data. Trusted hardware and trusted software can be combined to provide secure data processing. Trusted hardware and software are generally designed and tested to ensure the integrity and reliability of their source code, and their resistance to penetration. In contrast, untrusted hardware and untrusted software are generally not designed to an equally high level with regard to security precautions. Accordingly, when integrated into a computer system, those systems are often referred to as non-secure.

Secure PDA **100** utilizes secure user processor **102** comprised of trusted hardware (HW) and trusted software (SW) for securing data that is stored on the device. A user secure file system **103** is provided for storing classified data. A cryptographic engine **104** is provided with trusted hardware and trusted software for providing encryption and decryption services. A crypto secure file system **105** is used to store classified data and files used by the cryptographic engine **104**. A secure human/machine interface (HMI) **106** is also provided. However, for security reasons, PDA devices of this type generally do not include machine input/output (I/O) facilities. Thus PDA **100** does not have a USB port, wireless networking, or cellular telephone communications capabilities. PDA **100** can generally satisfy the requirements for accessing secure file systems. However, the operating system and applications can be expensive and unfamiliar to many users who more often utilize commercial-off-the-shelf (COTS) systems.

In contrast to the secure PDA in FIG. **1**, a commercial PDA/phone architecture is shown in FIG. **2**. The commercial PDA/phone **200** can include a non-secure processor **202** comprised of untrusted COTS microprocessor hardware and untrusted COTS software. A user non-secure file system **203** can be used for storing unclassified user files and data. The commercial PDA/phone will make use of COTS hardware and software to satisfy the processing and communications requirements of users. The commercial PDA/phone will make use of a conventional non-secure HMI **206**, and can include non-secure I/O circuitry **204**. The I/O circuitry **204** can include wired and/or wireless LAN transceivers, and cellular telephone transceiver circuitry. A suitable antenna or antennas **210** can be provided for any wireless applications. Audio interface circuitry can also be provided for headset **208**. Significantly, PDA **200** will not generally satisfy the requirements for accessing secure file systems. However, commercial PDA **200** benefits from the economy associated with use of COTS applications and a COTS operating system. Another advantage is that users tend to be well familiar with such operating systems and applications.

Turning now to FIG. **3**, there is shown an architecture for a mobile PDA computer system **300** that offers the combined advantages of secure PDA **100** and commercial PDA **200**. The architecture in FIG. **3** can include a secure processor **302** composed of trusted microprocessor hardware executing trusted operating system software and trusted application software. Secure processor **302** can have access to a secure file system **314**. Secure processor **302** receives user inputs and provides information to users through a secure HMI **308**. Secure processor **302** can also communicate audio information to and from headset **316**.

Non-secure processor **306** is also provided as part of PDA **300**. Non-secure processor **306** is composed of untrusted microprocessor hardware executing an untrusted operating system and untrusted application software. Non-secure processor **306** can store unclassified user files and data in a user non-secure file system **319**. Non-secure processor **306** is capable of receiving and transmitting data through I/O interface **312**, which can include wired and/or wireless LAN transceivers, cellular telephone transceiver circuitry and any other conventional data communication service. A suitable antenna or antennas **320** can be provided for any wireless applications. A user audio interface can be provided for audio communications, audio recording and listening to audio files. Non-secure processor **306** receives user inputs and provides information to users through a non-secure HMI **310**.

PDA **300** also includes a cryptographic engine **304**. The cryptographic engine is implemented with trusted software (operating system and application software) and trusted microprocessor hardware. The cryptographic engine is provided for encrypting and decrypting classified data. A crypto

secure file system **317** is provided for storing classified data and files used by cryptographic engine **304**. A first data communication link **303** is provided for communicating classified data between the secure processor **302** and the cryptographic engine **304**. A second data communication link **305** is provided for communicating encrypted classified data between the non-secure processor **306** and the cryptographic engine. Data communicated between secure processor **302** and cryptographic engine **304** will be encrypted before being passed to the non-secure processor **306**. In contrast, data communicated between non-secure processor **306** and cryptographic engine **304** can be unencrypted unclassified data in some instances and encrypted classified data in other instances. Still, the invention is not limited with regard to the specific type of data that is communicated on the first and second data links.

The first and second data communication links can be any suitable type serial or parallel type data channels. For example, if the communication link is a parallel type data link then it can conform to any of a number of well known bus standards, including without limitation ISA, EISA, VESA, PCI, EMIF and so on. Alternatively, if a serial data channel is used, then it can be an 12C, SPI, Microwire, Maxim or other type serial data bus.

A PDA computer architecture as show in FIG. **3** can offer several important advantages. One basic advantage of the foregoing arrangement is that it overcomes some limitations of conventional secure and non-secure PDAs. For example, the system can still offer all of the benefits of conventional commercial PDA devices. Such features can include familiar and inexpensive COTS operating systems and applications. Such COTS operating systems and applications can be used with the non-secure processor **306**. The PDA **300** also offers the benefit of wired and wireless LAN communication services, cellular telephone services and so on. In addition to these features, the PDA architecture shown in FIG. **3** can permit users to access to a secure file system. The file system can be maintained by secure processor **302** in a data store.

Referring now to FIG. **4**, there is shown a more detailed block diagram of a portion of the PDA **300** that includes non-secure processor **306**. As noted above, non-secure processor **306** can be comprised of untrusted processor hardware. For example, the untrusted processor hardware can be any one of a variety of well known COTS processors that are widely available. For example, the un-trusted processor hardware can be selected from the StrongARM or XScale processors (e.g., SA-110 or PXA270) available from Intel Corp. of Santa Clara, Calif., the i.MX or Dragonball family of processors available from Freescale Semiconductor, Inc. of Austin, Tex., or the OMAP family of processors offered for sale by Texas Instruments of Dallas, Tex.

According to one embodiment, non-secure processor **306** can also be comprised of an untrusted COTS operating system. For example any of a variety of well known COTS operating systems suitable for use in a PDA can be used for this purpose. According to one embodiment, the non-secure processor **306** can utilize the Windows CE operating system that is made available by Microsoft Corporation of Redmond, Wash. However, the invention is not limited in this regard and other types of untrusted operating systems can also be used.

Non-secure processor **306** can communicate with one or more subsystem components including data store **402**. Data store **402** can include flash memory, read-only memory (ROM), dynamic random access memory (DRAM). The untrusted operating system for the non-secure processor can be stored in non-volatile memory in data store **402** or flash EEPROM **404**. Application software can be loaded in flash memory or DRAM as needed.

As shown in FIG. **4**, I/O interface **312** can include wired connectivity block **406** for USB or other wired connectivity services. Wireless connectivity block **408** can include any wireless transceiver system now known or known in the future for communicating voice and/or data. For example, the wireless connectivity block **408** can be any suitable wireless LAN transceiver system. According to one embodiment of the invention, wireless connectivity block **408** can be configured for operation in accordance with any one of the 802.11 family of wireless network standards. However the invention is not limited in this regard. Instead, any other wireless networking standard can also be implemented in accordance with the inventive arrangements. Further, wireless connectivity block **408** can also comprise cellular telephone transceiver circuitry. For example, the cellular telephone transceiver circuitry can be designed to operate using any one of a variety of well known cellular telephone transmission protocols such as TDM, GSM, or CDMA.

Additional sub-systems connected to non-secure processor **306** can include audio interface **410**. Audio interface **410** can include at least one suitable audio codec, analog to digital and digital to analog conversion circuitry, as well as any necessary audio amplifier circuitry (not shown). Audio interface **410** can also include any other circuitry necessary to allow PDA **300** to output MP3 audio associated with the non-secure processor **306**.

In the event that wireless input/output subsystem **312** includes cellular telephone transceiver circuitry, then the audio interface **410** can include a voice codec that can provide the user audio interface for that application. In particular, the voice codec can code voice signals received from a microphone associated with headset **318**. Similarly, the voice codec can decode voice signals received via wireless connectivity block **408** and output such decoded audio to an earphone associated with headset **318**. Still, it should be understood that the invention is not limited to any particular arrangement with regard to audio interface **410**. Audio interfaces for cellular telephones and MP3 audio playback are well known in the art and all such arrangements are contemplated for audio interface **410** within the scope of the present invention.

Non-secure processor **306** can interface with a user through non-secure HMI **310**. Non-secure HMI **310** can include a conventional color display **416** and touch screen controller **414**. Non-secure HMI **206** can also include a keypad/pointing device **412**. HMI interfaces of the type described herein are well known in the art. In this regard it should be understood that the non-secure HMI interface is not limited to the specific embodiments shown. Instead, any other suitable non-secure HMI interface can be used for this purpose.

Referring now to FIG. **5**, there is shown a more detailed block diagram of the portion of PDA **300** including secure processor **302**. Secure processor **302** can be custom-designed processor or can also be one of a variety of well known COTS processors that are widely available. Regardless of whether the secure processor **302** is comprised of custom components, COTS components, or a mixture of custom and COTS components, the secure processor must be designed and developed utilizing trusted methods and techniques to ensure the integrity and reliability of the device, and its resistance to penetration. For example, the secure processor **302** can be housed inside a physical barrier that will detect any attempt to open the enclosure and automatically zeroize any stored sensitive/classified information contained within. The secure processor **302** can also be housed inside an enclosure that

provides radio frequency (RF) shielding to guard against radiating sensitive/classified information.

Secure processor **302** will also have trusted operating system software and trusted application software. Trusted software is designed and tested to ensure the integrity and reliability of the code, and its resistance to penetration. For example, trusted software must be developed utilizing trusted techniques, which may include peer reviews, testing of all paths through the control logic, and in some cases, a mathematical proof of correctness.

Secure processor **302** can communicate with one or more subsystem components including data store **502**. Data store **502** can include flash memory, read-only memory (ROM), dynamic random access memory (DRAM). The trusted operating system used in secure processor **302** can be stored in non-volatile memory in data store **502** or flash EE PROM **504**. Application software can be loaded in flash memory or DRAM as needed. Additional sub-systems connected to secure processor **302** can include audio interface **506**.

Audio interface **506** can include at least one suitable audio codec, analog to digital and digital to analog conversion circuitry, as well as any necessary audio amplifier circuitry (not shown). Audio interface **506** can also include any other circuitry necessary to allow PDA **300** to output MP3 audio associated with the secure processor **302**. In the event that wireless input/output subsystem **312** includes cellular telephone transceiver circuitry, then the audio interface **506** can include a voice codec that can provide the user audio interface for that application. In particular, the voice codec can code voice signals received from a microphone associated with headset **316**. Similarly, the voice codec can decode voice signals received via wireless connectivity block **408** and output such decoded audio to an earphone associated with headset **316**. Still, it should be understood that the invention is not limited to any particular arrangement with regard to audio interface **506**. Audio interfaces for cellular telephones and MP3 audio playback are well known in the art and all such arrangements are contemplated for audio interface **506** within the scope of the present invention.

Secure processor **302** can also communicate with secure HMI **308**. Secure HMI devices are known in the art and typically can include one or more features to ensure trusted communications between the user and the secure processor **302**. The secure HMI **308** can provide a trusted path to applications executing on secure processor **302**. Consequently, secure HMI **308** can prevent invasive or unauthorized applications from monitoring user inputs and system outputs.

According to one embodiment of the invention, the secure HMI **308** can be at least partially contained within a shielded enclosure. Moreover, the power supply lines for the secure HMI **308** can be filtered to ensure that signals associated with secure processor **302** are not communicated along the power supply lines back to the non-secure processor **306**. The secure HMI **308** can also be designed to prevent a user from being misled about which application is actually in use. For example, this can be accomplished by means of highly distinctive and easily recognized visual display indications that cannot be obstructed. Such indicators can assure the user regarding the identity of the application with which the user is working. Secure HMI features of this type are implemented in a variety of ways that are known to those skilled in the art.

Referring now to FIG. **5**, it can be observed that the secure HMI **308** can be comprised of several components. For example, secure HMI **308** can include one or more input devices which allow a user to input control commands and input data. According to one embodiment, these input devices can include a pointing keypad/pointing device **508** and a touch screen controller **510**. However, the invention is not limited in this regard. The secure HMI **308** can also include a display **512**, which can present alphanumeric and graphical data. The display **512** can be a color or monochrome type display. Further, one or more data ports (not shown) can be provided as part of the human/machine interface. The data ports can be any type of wired data interface. According to one embodiment, the data ports can conform to the well known USB standard. The data ports can be used for input and output of data. The data ports can also be used for connecting certain peripheral devices to the PDA **300**. For example, the data ports can be used for connecting an external keyboard to the PDA **300**.

Referring now to FIG. **6**, there is shown a more detailed block diagram of cryptographic engine **304**. Cryptographic engine **304** can include a cryptographic processor **602** and a cryptographic file system **604** maintained in a data store. Cryptographic engine **304** can be one of several available cryptographic engines. According to one embodiment, the cryptographic engine can be a Sierra II Crypto processor which is available from Harris Corporation of Melbourne, Fla. The cryptographic engine can include configurable key lengths and can be programmed with one or more encryption algorithms. As illustrated in FIG. **6**, cryptographic engine **304** can include several control and data ports including a crypto ignition key port, a key and certificate fill port, a zeroize switch, and a software load port. The software load port can be used for loading software for executing on the cryptographic engine **304** and for loading software used by secure processor **302**.

The cryptographic file system **604** can be used to store cryptographic algorithms, crypto keys and certificates, audit data, policy profile, and any other information necessary for the operation of the cryptographic engine. The cryptographic engine **304** can also include one or more security features. For example, the cryptographic engine **304** can include a secure certified operating environment, security auditing, security policy enforcement, file integrity checking and/or trusted boot logic. Cryptographic file system **604** can be implemented in flash/ROM/DRAM **603** and/or EE PROM **605**.

As shown in FIG. **6**, the cryptographic engine **304** can be responsive to one or more control signals from secure processor **302** and non-secure processor **306** to provide various encryption functions. For example, according to one aspect of the invention, the cryptographic engine can provide an encryption/decryption function for data communicated between the secure and non-secure processors. The encryption function can be implemented with or without packet header bypass.

The functions of the cryptographic engine **304** can be responsive to crypto control signals received from the secure processor **302** and non-secure processor **306** via the crypto interfaces **606**, **608**. For example, any data of a sensitive nature that is transferred from the secure processor to the cryptographic engine **304** must be encrypted before being transferred to the non-secure processor.

With the PDA architecture as described herein in relation to FIG. **3**, the user is capable of storing, processing, and communicating classified as well as unclassified data. Unclassified data storage and user processing of unclassified data can be performed by non-secure processor **306**. The architecture provides for the use of untrusted COTS operating systems and COTS applications for the non-secure user. The use of COTS hardware and software for the non-secure processor provides the users with familiar user interfaces expected by the user community. In contrast, classified data storage and user processing of classified data can be provided using the secure

processor **302** and a secure file system **314** accessed by secure processor **302**. Any data of a sensitive nature transferred from the secure processor to the non-secure processor can be encrypted by the cryptographic engine **304**. An advantage of the foregoing architecture is that it (1) provides for physical separation of classified data from data which is unclassified or encrypted/classified data, and (2) provides secure access to sensitive files.

The foregoing arrangement also facilitates a secure/non-secure PDA architecture that provides for wired and wireless communications capabilities. Unclassified data can be transmitted using conventional wired connectivity **406** or wireless connectivity **408**. Significantly, however, data that is of a sensitive nature can also be transmitted. For example, encrypted data stored in a secure file system associated with secure processor **302** can be communicated from secure processor **302** to non-secure processor **306**, without being unencrypted. Unencrypted data can be encrypted by cryptographic engine **304** before being communicated from the secure processor **302** to the non-secure processor **306**. Thereafter, the encrypted data can be communicated over-the-air by means of non-secure processor **306** and wired connectivity **408** using COTS software applications. Likewise, text messages and other communications originating from the secure HMI **308** can be encrypted when passed from secure processor **302** to non-secure processor **306**. Consequently, any of the wired connectivity **406** or wireless connectivity services **406** can be used to communicate the data to third parties.

Another advantage of the foregoing arrangement is that it allows a user with classified and unclassified voice communications to take advantage of the wireless connectivity **408** for telecommunications services. For example, if the PDA **300** is equipped with a cellular telephone transceiver or other wireless transceiver that can be used for voice communications, then a user can plug in a headset **316** to provide encrypted communications with third parties. Audio data communicated to secure processor **302** by headset **316** can be encrypted by cryptographic engine **304** before ever passing to the non-secure side of the architecture of PDA **300**. Likewise, classified audio communications can be received in an encrypted state and can remain encrypted until passing to the secure processor side of the PDA **300**. Unclassified voice communications can be conducted using headset **318** and non-secure processor **306** in the conventional manner. However, under no circumstances will classified audio information be communicated to the non-secure audio processing hardware so it cannot be inadvertently transmitted in an unencrypted state.

I claim:

1. A computer system, comprising:

a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine;

said secure user processor comprising

a trusted microprocessor,

a trusted operating system executing on said trusted microprocessor, and

a trusted application software executing on said trusted microprocessor;

said non-secure user processor comprising

an untrusted microprocessor,

an untrusted operating system executing on said untrusted microprocessor, and

an untrusted application software executing on said untrusted microprocessor;

said cryptographic engine configured for encrypting any data communicated from said secure user processor to said non-secure user processor, comprising

a trusted cryptographic processor, and

a trusted operating system executing on said trusted cryptographic processor;

a first data communication link communicating data between said secure processor and said cryptographic engine;

a second data communication link communicating data between said non-secure processor and said cryptographic engine;

a secure human/machine interface configured for enabling bi-directional communication of classified information exclusively between a user and said secure user processor; and

a non-secure human/machine interface distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure user processor;

wherein said communications transceiver is operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device.

2. The computer system according to claim **1**, wherein said secure human/machine interface comprises at least one input device to allow said user to control the secure user processor.

3. The computer system according to claim **2**, wherein said secure human/machine interface comprises at least one output device to allow the secure user processor to inform said user.

4. The computer system according to claim **1**, wherein said non-secure human/machine interface comprises at least one input device to allow said user to control the non-secure user processor.

5. The computer system according to claim **4**, wherein said non-secure human/machine interface comprises at least one output device to allow the non-secure user processor to inform said user.

6. The computer system according to claim **1**, wherein said communications transceiver is selected from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver.

7. The mobile PDA computer system according to claim **1**, further comprising a first file system exclusively accessible to said secure user processor for storing classified data and a second file system for storing unclassified data, said second file system distinct from said first file system so as to provide physical separation of said classified data from said unclassified data within said portable mobile computing device.

8. A computer system, comprising:

a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine;

said secure user processor comprising

a trusted microprocessor,

a trusted operating system executing on said trusted microprocessor, and

a trusted application software executing on said trusted microprocessor;

said non-secure user processor comprising

an untrusted microprocessor,

an untrusted operating system executing on said untrusted microprocessor, and

an untrusted application software executing on said untrusted microprocessor;

said cryptographic engine configured for encrypting any data communicated from said secure user processor to said non-secure user processor, comprising

a trusted cryptographic processor, and

a trusted operating system executing on said trusted cryptographic processor;

a first data communication link communicating data between said secure processor and said cryptographic engine;

a second data communication link communicating data between said non-secure processor and said cryptographic engine; and

first and second audio interfaces, said first audio interface configured for communicating audio information to and from said secure user processor, and said second audio interface configured for communicating audio information to and from said non-secure user processor;

wherein said communications transceiver is operatively coupled to said non-secure user processor, is configured for communicating data external to said portable mobile computing device, and is selected from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver.

9. A computer system, comprising:

a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine,

said communications transceiver operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device,

said secure user processor comprising

a trusted microprocessor,

a trusted operating system executing on said trusted microprocessor, and

a trusted application software executing on said trusted microprocessor;

said non-secure user processor comprising

an untrusted microprocessor,

an untrusted operating system executing on said untrusted microprocessor, and

an untrusted application software executing on said untrusted microprocessor;

said cryptographic engine configured for encrypting data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptographic processor;

a first data communication link communicating data between said secure user processor and said cryptographic engine;

a second data communication link communicating data between said non-secure user processor and said cryptographic engine;

a secure human/machine interface communicatively coupled to said secure user processor and configured to enable bi-directional communication of classified information exclusively between a user and said secure user processor, at least a portion of said secure human/machine interface located in a physically secure enclosure; and

a non-secure human/machine interface communicatively coupled to said non-secure user processor and configured to enable bi-directional communication of unclassified information exclusively between said user and said non-secure user processor, said non-secure human/machine interface distinct from said secure human/machine interface.

10. The computer system according to claim **9**, wherein said non-secure user processor is operatively connected to said communications transceiver.

11. A computer system, comprising:

a portable mobile computing device including a secure user processor, a non-secure user processor, a communications transceiver, and a cryptographic engine, said communications transceiver operatively coupled to said non-secure user processor and configured for communicating data external to said portable mobile computing device,

said secure user processor comprising

a trusted microprocessor,

a trusted operating system executing on said trusted microprocessor, and

a trusted application software executing on said trusted microprocessor;

said non-secure user processor comprising

an untrusted microprocessor,

an untrusted operating system executing on said untrusted microprocessor, and

an untrusted application software executing on said untrusted microprocessor;

said cryptographic engine configured for encrypting data communicated from said secure user processor to said non-secure user processor, comprising a trusted cryptographic processor, and a trusted operating system executing on said trusted cryptophic processor;

a first data communication link communicating data between said secure user processor and said cryptographic engine;

a second data communication link communicating data between said non-secure user processor and said cryptographic engine;

a secure human/machine interface communicatively coupled to said secure user processor and configured to provide a user of said portable mobile computing device with access and control of said secure user processor;

a non-secure human/machine interface communicatively coupled to said non-secure user processor and configured to provide said user with access and control of said non-secure user processor, said non-secure human/machine interface distinct from said secure human/machine interface;

a first audio interface for communicating audio information to and from said secure user processor; and

a second audio interface for communicating audio information to and from said non-secure user processor.

12. A method for managing classified and unclassified data on a portable mobile computing device of a computer system, comprising:

processing said classified data exclusively using a secure processor of said portable mobile computing device, said secure processor comprising a trusted microprocessor and a trusted operating system executing on said trusted microprocessor;

processing unclassified data exclusively using a non-secure processor of said portable mobile computing device, said non-secure processor comprising an untrusted microprocessor and an untrusted operating system executing on said untrusted microprocessor;

communicating encrypted and decrypted classified data between said secure processor and a cryptographic

engine of said portable mobile computing device using a first data communication link;

communicating data from said secure processor and said cryptographic engine to said non-secure processor exclusively in an encrypted form using a second data communication link between said cryptographic engine and said non-secure processor;

communicating classified information to and from said secure processor using a secure human/machine interface that is configured for enabling bi-directional communication of classified information exclusively between a user and said secure processor; and

communicating unclassified information to and from said non-secure processor using a non-secure human/machine interface that is distinct from said secure human/machine interface and configured for enabling bi-directional communication of unclassified information exclusively between said user and said non-secure processor.

13. The method according to claim **12**, further comprising controlling said secure processor exclusively using said secure human/machine interface.

14. The method according to claim **12**, further comprising controlling said non-secure processor exclusively using a non-secure human/machine interface.

15. The method according to claim **12**, further comprising performing wireless data communication of unclassified data from said non-secure processor using a wireless communications transceiver.

16. The method according to claim **15**, further comprising communicating encrypted classified data from said secure processor using said wireless communications transceiver.

17. The method according to claim **15**, further comprising selecting said wireless communications transceiver from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver.

18. The method according to claim **12**, further comprising storing classified data in a first file system accessible only to said secure user processor and storing unclassified data in a second file system distinct from said first file system which is accessible to said non-secure user processor, thereby providing physical separation of said classified data from said unclassified data within said portable mobile computing device.

19. A method for managing classified and unclassified data on a portable mobile computing device of a computer system, comprising:

processing said classified data exclusively using a secure processor of said portable mobile computing device, said secure processor comprising a trusted microprocessor and a trusted operating system executing on said trusted microprocessor;

processing unclassified data exclusively using a non-secure processor of said portable mobile computing device, said non-secure processor comprising an untrusted microprocessor and an untrusted operating system executing on said untrusted microprocessor;

communicating encrypted and decrypted classified data between said secure processor and a cryptographic engine of said portable mobile computing device using a first data communication link;

communicating data from said secure processor and said cryptographic engine to said non-secure processor exclusively in an encrypted form using a second data communication link between said cryptographic engine and said non-secure processor;

performing wireless data communication of said unclassified data from said non-secure processor using a wireless communications transceiver;

selecting said wireless communications transceiver from the group consisting of a wireless LAN transceiver and a cellular telephone transceiver;

communicating classified audio information to and from said secure processor with a first audio interface; and

communicating unclassified audio information to and from said processor with a second audio interface distinct from said first audio interface.

* * * * *