

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7500587号
(P7500587)

(45)発行日 令和6年6月17日(2024.6.17)

(24)登録日 令和6年6月7日(2024.6.7)

(51)国際特許分類		F I	
G 0 1 S	11/08 (2006.01)	G 0 1 S	11/08
G 0 1 S	5/14 (2006.01)	G 0 1 S	5/14
H 0 4 W	4/02 (2018.01)	H 0 4 W	4/02
H 0 4 W	12/08 (2021.01)	H 0 4 W	12/08
H 0 4 W	12/122 (2021.01)	H 0 4 W	12/122
請求項の数 13 (全45頁) 最終頁に続く			
(21)出願番号	特願2021-548267(P2021-548267)	(73)特許権者	590000248
(86)(22)出願日	令和2年2月17日(2020.2.17)		コーニンクレッカ フィリップス エヌ
(65)公表番号	特表2022-520865(P2022-520865		ヴェ
	A)		Koninklijke Philips
(43)公表日	令和4年4月1日(2022.4.1)		N. V.
(86)国際出願番号	PCT/EP2020/054029		オランダ国 5 6 5 6 アーヘー アイン
(87)国際公開番号	WO2020/169505		ドーフエン ハイテック キャンパス 5 2
(87)国際公開日	令和2年8月27日(2020.8.27)		High Tech Campus 52,
審査請求日	令和5年2月15日(2023.2.15)		5 6 5 6 AG Eindhoven, N
(31)優先権主張番号	19158080.2		etherlands
(32)優先日	平成31年2月19日(2019.2.19)	(74)代理人	110001690
(33)優先権主張国・地域又は機関	欧州特許庁(EP)		弁理士法人M&Sパートナーズ
		(72)発明者	バーンセン ヨハネス アーノルドス コ
			ーネリス
			オランダ国 5 6 5 6 アーエー アイン
			最終頁に続く

(54)【発明の名称】 信用される距離測定のためのシステム

(57)【特許請求の範囲】

【請求項1】

第1のデバイスとして動作するデバイスと、無線通信のための第2のデバイスとの間の無線通信を介して距離を測定するための当該デバイスであって、

前記無線通信は、前記第1のデバイスにおける測定メッセージの到達時刻に基づいて前記第1のデバイスと前記第2のデバイスとの間の距離を測定するための測距プロトコルを含み、前記測距プロトコルは、前記第2のデバイスによって前記測定メッセージを送信することを含み、

前記デバイスは、

メッセージを送信及び受信するための第1のトランシーバと、第1のメッセージプロセッサとを備え、

前記第1のメッセージプロセッサは、

前記測距プロトコルに従って前記測定メッセージを処理することと、

第1のデバイスにおける前記測定メッセージの第1の到達時刻を決定することと、

前記第1の到達時刻に基づいて前記第1のデバイスと前記第2のデバイスとの間の第1の距離を決定することと

を行い、

前記第1のメッセージプロセッサは、第3のデバイスと通信するように構成されており、前記第3のデバイスは、前記第1のデバイスからの信用される距離をおいて配置されている協働デバイスとして動作し、

決定された前記距離を評価するために、

前記協働デバイスからサポートデータを受信することであって、前記サポートデータは、前記協働デバイスにおける第1のメッセージの第3の到達時刻に基づく、受信することと、

前記サポートデータを使用して前記第3のデバイスと前記第2のデバイスとの間の第3の距離を得ることと、

前記第1の距離、前記信用される距離及び前記第3の距離に関する検証テストを実施することであって、前記検証テストは、これらの距離が、前記第1のデバイス、前記第2のデバイス及び前記協働デバイスの有効な空間的配置に対応するときに、前記第1の距離を信頼可能であるとして許容する、検証テストを実施することと

10

を行う、デバイスにおいて、

前記測距プロトコルは、鍵データに基づいて暗号によって保護されているメッセージを交換することを含み、前記第1のメッセージプロセッサは、前記第3のデバイスのメッセージプロセッサが前記測距プロトコルに従って前記メッセージを暗号論的に処理することを可能にするために、前記協働デバイスと前記鍵データを共有する、デバイス。

【請求項2】

前記検証テストは、前記有効な空間的配置に関する余弦法則チェック又は三角不等式チェックを含む、請求項1に記載のデバイス。

【請求項3】

前記第1のメッセージプロセッサは、前記測距プロトコルに従って前記信用される距離を決定する、請求項1又は2に記載のデバイス。

20

【請求項4】

前記デバイスは、前記到達時刻を決定するための時間基準を提供するためのクロックユニットを備え、前記第1のメッセージプロセッサは、前記時間基準を、前記協働デバイス内の対応するクロックユニットと同期させる、請求項1から3のいずれか一項に記載のデバイス。

【請求項5】

前記測距プロトコルは、前記第1のデバイスが、開始デバイスとして動作し、前記第2のデバイスに開始メッセージを送信することを含み、一方、前記開始メッセージが受信されると、前記第2のデバイスは、前記測定メッセージを送信する必要があり、前記第1のメッセージプロセッサは、

30

前記第3のデバイスが距離測定のために前記開始デバイスとして動作することを可能にするために、前記第3のデバイスと役割変更データを交換し、

前記第3のデバイスは、前記役割変更データを受信すると、

第2の測定メッセージに基づいて前記測距プロトコルに従って前記第3のデバイスと前記第2のデバイスとの間の第3の距離を得ることと、

前記第3の距離を示す第3のサポートデータを前記第1のデバイスに転送することとを行い、

一方、前記第1のメッセージプロセッサは、

前記第1のデバイスにおいて前記第2の測定メッセージを受信するときの前記第1のデバイスと前記第2のデバイスとの間の第2の距離を決定することと、

40

前記第3のデバイスから前記第3のサポートデータを受信することと、

前記第2の距離及び前記第3のサポートデータも使用して前記検証テストを実施することと

を行う、請求項1から4のいずれか一項に記載のデバイス。

【請求項6】

前記第3のデバイスのメッセージプロセッサは、

前記第2のデバイスから受信される少なくとも1つのメッセージの第3の信号強度を決定し、

第3の信号強度データを、前記第1のデバイスへの前記サポートデータに含め、

50

前記第 1 のメッセージプロセッサは、

前記第 2 のデバイスから受信される少なくとも 1 つのメッセージの第 1 の信号強度を決定し、

前記第 1 の信号強度及び前記第 3 の信号強度を、決定された前記距離におけるそれぞれの予測信号強度と比較することによって、前記決定された距離が信頼可能であるか否かを検証する、請求項 1 から 5 のいずれか一項に記載のデバイス。

【請求項 7】

前記第 1 のメッセージプロセッサは、前記決定された距離が信頼可能でないという評価を受けて、

前記第 2 のデバイスに対する異なるセキュリティプロトコルを実行することを要求することと、

異なる測距プロトコル及び／又は異なるタイプの無線通信を使用したさらなる距離測定を要求することと、

前記第 1 のデバイス内の少なくともいくつかのデータ及び／又は少なくとも 1 つの機能に対するアクセスを拒否又は制限することと

のうちの少なくとも 1 つを行う、請求項 1 から 6 のいずれか一項に記載のデバイス。

【請求項 8】

距離を信頼可能に測定するためのシステムであって、請求項 1 から 7 のいずれか一項に記載のデバイスと、前記第 3 のデバイスと、前記第 1 のデバイスから又は前記第 3 のデバイスからの第 2 の信用される距離において配置されている、第 2 の協働デバイスとして動作する第 4 のデバイスとを備え、

前記第 4 のデバイスは、

メッセージを受信するための第 4 の無線レシーバと、第 4 のメッセージプロセッサとを有し、

前記第 4 のメッセージプロセッサは、

前記第 4 のデバイスにおける前記測定メッセージの第 4 の到達時刻を決定することと、

前記第 4 の到達時刻に基づく第 4 のサポートデータを前記第 1 のデバイスに転送することとを行い、

前記第 1 のメッセージプロセッサは、

前記第 2 の協働デバイスから前記第 4 のサポートデータを受信することと、

前記第 4 のサポートデータを使用して前記第 4 のデバイスと前記第 2 のデバイスとの間の第 4 の距離を得ることと、

前記第 2 の信用される距離及び前記第 4 の距離も使用して前記検証テストを実施することとを行う、システム。

【請求項 9】

前記第 1 のメッセージプロセッサは、

前記第 1 のデバイス、前記第 2 のデバイス及び前記第 3 のデバイスの第 1 の空間的配置に関する第 1 の三角不等式と、前記第 1 のデバイス、前記第 2 のデバイス及び前記第 4 のデバイスの第 2 の空間的配置に関する第 2 の三角不等式との組み合わせを使用して前記検証テストを実施すること、又は

前記第 1 の空間的配置による前記第 2 のデバイスの第 1 の位置が前記第 2 の空間的配置による前記第 2 のデバイスの第 2 の位置に対応するか否かを検証すること、又は

前記決定された距離のすべてがゼロよりも大きいかな否かを決定するための非一貫性チェックを使用して前記検証テストを実施すること、又は

前記第 3 のデバイスから前記第 1 のデバイスへの線と、前記第 4 のデバイスから前記第 1 のデバイスへの線との間の信頼される角度が少なくとも 90 度になるように、前記第 3 のデバイス及び前記第 4 のデバイスが配置される構成に基づいて前記検証テストを実施すること、又は

前記第 3 のデバイス及び前記第 4 のデバイスが前記第 1 のデバイスに関して互いに対向して配置される構成に基づいて前記検証テストを実施すること、又は

10

20

30

40

50

前記第 2 の信用される距離が前記信用される距離に対応する構成に基づいて前記検証テストを実施することを行う、請求項 8 に記載のシステム。

【請求項 10】

前記システムは、さらなる協働デバイスとして動作する少なくとも 1 つのさらなるデバイスを備え、前記第 3 のデバイス、前記第 4 のデバイス及び前記少なくとも 1 つのさらなるデバイスは、一平面内で、多角形のエッジに配置され、前記第 1 のデバイスは前記多角形の内部にあり、前記第 1 のメッセージプロセッサは、

少なくとも 2 つの空間的配置に関する三角不等式の組み合わせを使用して前記検証テストを実施し、各配置は、前記第 2 のデバイスと、前記第 1 のデバイス及び前記協働デバイスのセットのうちの 2 つのデバイスとを含む、請求項 8 又は 9 に記載のシステム。

10

【請求項 11】

第 1 のデバイスと第 2 のデバイスとの間の無線通信を介して距離を測定するための方法であって、

前記無線通信は、前記第 1 のデバイスにおける測定メッセージの到達時刻に基づいて前記第 1 のデバイスと前記第 2 のデバイスとの間の距離を測定するための測距プロトコルを含み、前記測距プロトコルは、前記第 2 のデバイスによって前記測定メッセージを送信することを含み、

前記方法は、

前記第 1 のデバイスの第 1 のメッセージプロセッサが、前記第 1 のデバイスにおける前記測定メッセージの第 1 の到達時刻に基づいて前記第 1 のデバイスと前記第 2 のデバイスとの間の第 1 の距離を得るステップと、

20

前記第 1 のメッセージプロセッサが、第 3 のデバイスと通信するステップと

を有し、前記第 3 のデバイスは、前記第 1 のデバイスからの信用される距離をおいて配置されている協働デバイスとして動作し、

前記第 3 のデバイスは、

前記第 3 のデバイスにおける前記測定メッセージの第 3 の到達時刻を決定することと、

前記第 3 の到達時刻に基づくサポートデータを提供することと

を行い、

前記方法は、決定された前記距離を評価するために、

前記第 1 のメッセージプロセッサが、前記サポートデータを使用して前記第 3 のデバイスと前記第 2 のデバイスとの間の第 3 の距離を得るステップと、

30

前記第 1 のメッセージプロセッサが、前記第 1 の距離、前記信用される距離及び前記第 3 の距離に関する検証テストを実施するステップであって、前記検証テストは、前記距離が、前記第 1 のデバイス、前記第 2 のデバイス及び前記協働デバイスの有効な空間的配置に対応するときに、前記第 1 の距離を信頼可能であるとして許容する、検証テストを実施するステップと

を有する、方法において、

前記測距プロトコルは、鍵データに基づいて暗号によって保護されているメッセージを交換することを含み、前記第 1 のメッセージプロセッサは、前記第 3 のデバイスのメッセージプロセッサが前記測距プロトコルに従って前記メッセージを暗号論的に処理することを可能にするために、前記協働デバイスと前記鍵データを共有する、方法。

40

【請求項 12】

第 1 のデバイスと第 2 のデバイスとの間の無線通信を介した距離測定において協働デバイスとして動作するための方法であって、

前記協働デバイスは、前記第 1 のデバイスから信用される距離に位置し、

前記無線通信は、前記第 1 のデバイスにおける測定メッセージの到達時刻に基づいて前記第 1 のデバイスと前記第 2 のデバイスとの間の距離を測定するための測距プロトコルを含み、前記測距プロトコルは、前記第 2 のデバイスによって前記測定メッセージを送信することを含み、

前記第 1 のデバイスは、

50

前記第 1 のデバイスにおける前記測定メッセージの第 1 の到達時刻に基づいて前記第 1 のデバイスと前記第 2 のデバイスとの間の第 1 の距離を取得し、

前記方法は、

前記協働デバイスが、前記協働デバイスにおける前記測定メッセージの第 3 の到達時刻を決定するステップと、

前記協働デバイスが、前記第 3 の到達時刻に基づくサポートデータを提供するステップと
前記第 1 のデバイスの第 1 のメッセージプロセッサが、前記サポートデータを使用して前記協働デバイスと前記第 2 のデバイスとの間の第 3 の距離を得るステップと、

前記第 1 のメッセージプロセッサが、前記第 1 の距離、前記信用される距離及び前記第 3 の距離に関する検証テストを実施するステップであって、前記検証テストは、これらの距離が、前記第 1 のデバイス、前記第 2 のデバイス及び前記協働デバイスの有効な空間的配置に対応するときに、前記第 1 の距離を信頼可能であるとして許容する、検証テストを実施するステップと

を行う、方法において、

前記測距プロトコルは、鍵データに基づいて暗号によって保護されているメッセージを交換することを含み、前記第 1 のメッセージプロセッサは、前記協働デバイスのメッセージプロセッサが、前記測距プロトコルに従って前記メッセージを暗号論的に処理することを可能にするために、前記協働デバイスと前記鍵データを共有する、方法。

【請求項 1 3】

ネットワークからダウンロード可能であり、並びに／又は、コンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶されるコンピュータプログラムであって、前記コンピュータプログラムは、コンピュータ上で実行されるときに、請求項 1 1 又は 1 2 に記載の方法を実施するためのプログラムコード命令を含む、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、第 1 のデバイスとして動作するデバイスと無線通信のための第 2 のデバイスとの間の無線通信を介した距離測定のためのデバイスに関し、無線通信は、第 1 のデバイスにおける測定メッセージの到達時刻に基づいて第 1 のデバイスと第 2 のデバイスとの間の距離を測定するための測距プロトコルを含み、プロトコルは、第 2 のデバイスによって測定メッセージを送信することを含む。本発明は、さらに、距離測定のための方法、及び、デバイス又はサーバ内で使用するためのコンピュータプログラム製品に関する。

【0002】

本発明は、概して位置測定システムの分野に関し、より詳細には、距離測定値を検証するための様々なデバイス及び方法並びに対応するコンピュータプログラム製品を提供する。

【背景技術】

【0003】

位置認識サービスの必要性が、屋内領域において存在する。例えば、病院、大学、駐車場、ショッピングモール、及び／又はオフィスなどの大型屋内複合施設において、近距離にあるモバイルデバイスに無線サービスが提供される。屋内位置測定システムが、消費者（以下、エンドユーザ）にサービスを提供し、サービスは、エンドユーザが最終的に依拠するものである。そのような位置測定に基づくサービスは、サービスを提供するデバイスの近くにある、すなわち、サービスを提供するデバイスまで限定された距離にあるデバイスにしか提供されない。さらなる例において、電子無線自動車ドア鍵は、ドアを開くことが可能になる前に、自動車の近くになければならない。不正なドア鍵が、自動車から本来必要である近さよりもはるかに遠くにあるときにドアを開くことができるように、距離測定プロトコルを改ざんする。

【0004】

したがって、距離測定が信頼可能であることが重要である。このコンテキストにおいて

、信頼可能とは、応答デバイスまでの実際の距離とは異なる距離を意図的に生じるように改ざん又は偽装された距離又は到達時刻データとは反対に、応答デバイスが、測定されたものとしての信頼可能で正しい距離又は到達データを提供することを意味する。

【0005】

距離測定のための既知のシステムは、IEEE 802.11において定義されている無線通信のためのプロトコルのバージョンにおいて最近開発されている。参考文献[802.11]を参照されたい。このバージョンは、2つのデバイス間の距離を決定するための測距プロトコルを含み、正確な距離測定、及び、1メートルまで又はさらにはより細かい分解能でデバイスの位置を決定することを可能にする。ファインタイミング測定手順(FTM: Fine Timing Measurement)と呼ばれる測距プロトコルが、[802.11] Chapter 10.24.6において定義されており、信号の往復時間(RTT)を決定するための測定メッセージの到達時刻を正確に測定し、送信タイミングと組み合わせたメッセージの測定到達時刻に基づいて距離を導出する。例えば、実質的に光速で自由大気内を伝播する無線信号を仮定すると、この放射線が1メートルの距離をカバーするには3.3 nsかかり、一方で、Wi-Fi(登録商標)ステーションは、約0.1 nsの時間粒度に達することが可能である。

10

【0006】

この応用形態は、測距プロトコルの分野内であることに留意されたい。これらは、電磁放射線が送信機と受信器との間を進行するのにかかる時間を測定する飛行時間測定として知られているものに対応する。それらは、IPデータパケットがネットワーク内でソースデバイスからシンクデバイスへと遷移するのにかかる時間を測定し、そのような遷移は複数の中間デバイスを含む、ping時間としても知られるIP/HTTPプロトコルにおいて実施される距離測定とは根本的に異なる。

20

【0007】

2つのデバイスが到達時刻測定値に基づいて距離を決定するためには、それらのデバイスは、測距プロトコルに従って動作する必要がある。例えば、開始無線デバイスが、往復時間測定を開始することを求める要求を開始する。応答デバイスが、メッセージの送信と要求の受信との間の間隔を決定し、この時間間隔を開始デバイスに送信する。

【0008】

しかしながら、虚偽のデータを送信することによって、デバイスは実際には、現実にもうであるよりも近い又は遠いと主張することができる。また、測定メッセージは、例えば、タイミンググリッドに従ってなど、所定の時点において送信される必要がある。悪意のあるデバイスが、測定メッセージを意図的に異なる時点において送信する。そのような悪意のある挙動は、開始デバイスが、決定された距離/位置情報が正確であると信頼する場合に、位置に基づくサービスの悪用の可能性をもたらし得る。例えば、位置に基づくサービスが、何らかのトランザクションを自動的に開始する。

30

【0009】

そのため、既知のシステムにおいて、測定値又は受信距離データは、改ざんされている場合があり、したがって完全に信頼することはできない。

【発明の概要】

40

【発明が解決しようとする課題】

【0010】

802.11の時間測定(TM)又は精細時間測定(FTM: Fine Time Measurement)方法を使用して第2のデバイスまでの距離を測定する第1のデバイスは、偽装を行うにあたって現実にもうであるのとは異なる(特により小さい距離に現れることを所望する)悪意のあるデバイスによる偽装到達時刻(TOA)及び偽装出発時刻(TOD)から自身を保護するように試行する。

【0011】

そのような挙動に対抗するために、距離測定システムは、第3のデバイスを伴い、第3のデバイスは同じく、第3のデバイスと、悪意のあるものである可能性がある第2のデバ

50

イスとの間の第2の距離を決定するための距離測定を実施する。両方の距離を比較し、第1のデバイスと協働デバイスとの間の距離を理解し、信頼することによって、両方の決定された距離に関する検証を実施する。しかしながら、悪意のあるデバイスが、検証テストに合格するように、両方の距離測定値を改ざんすることは、より複雑ではあるが、依然として可能である。

【0012】

本発明の目的は、到達時刻に基づく距離測定をより信頼可能に行うためのシステムを提供することである。この目的のために、添付の特許請求の範囲において定義されているものとしてのデバイス及び方法が提供される。

【課題を解決するための手段】

【0013】

本発明の第1の態様によれば、第1のデバイスとして動作するデバイスと無線通信のための第2のデバイスとの間の無線通信を介した距離測定のための当該デバイスが提供され、無線通信は、第1のデバイスにおける測定メッセージの到達時刻に基づいて第1のデバイスと第2のデバイスとの間の距離を測定するための測距プロトコルを含み、プロトコルは、第2のデバイスによって測定メッセージを送信することを含み、

デバイスは、

メッセージを送信及び受信するための第1のトランシーバと、第1のメッセージプロセッサとを備え、

第1のメッセージプロセッサは、

測距プロトコルに従ってメッセージを処理することと、

第1のデバイスにおける測定メッセージの第1の到達時刻を決定することと、

第1の到達時刻に基づいて第1のデバイスと第2のデバイスとの間の第1の距離を決定することと

を行うように構成され、

第1のメッセージプロセッサは、第3のデバイスと通信するように構成されており、第3のデバイスは、第1のデバイスから信用される距離において配置されている協働デバイスとして動作し、

決定された距離を評価するために、

協働デバイスからサポートデータを受信することであって、サポートデータは、協働デバイスにおける第1のメッセージの第3の到達時刻に基づく、受信することと、

サポートデータを使用して第3のデバイスと第2のデバイスとの間の第3の距離を得ることと、

第1の距離、信用される距離及び第3の距離に関する検証テストを実施することであって、検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する、検証テストを実施することと

を行う。

【0014】

さらなる態様によれば、第1のデバイスと第2のデバイスとの間の無線通信を介して距離を測定するための方法が提供され、方法は、

第1のデバイスにおける測定メッセージの第1の到達時刻に基づいて第1のデバイスと第2のデバイスとの間の第1の距離を得るステップと、

第3のデバイスと通信するステップと

を有し、第3のデバイスは、第1のデバイスから信用される距離において配置されている協働デバイスとして動作し、

第3のデバイスは、

第3のデバイスにおける測定メッセージの第3の到達時刻を決定することと、

サポートデータを提供することであって、サポートデータは、第3の到達時刻に基づく、提供することと

10

20

30

40

50

を行うように構成されており、

方法は、決定された距離を評価するために、

サポートデータを使用して第3のデバイスと第2のデバイスとの間の第3の距離を得るステップと、

第1の距離、信用される距離及び第3の距離に関する検証テストを実施するステップであって、検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する、検証テストを実施するステップと

を有する。

【0015】

さらなる態様によれば、第1のデバイスと第2のデバイスとの間の無線通信を介した距離測定において協働デバイスとして動作するための方法が提供され、協働デバイスは、第1のデバイスから信用される距離において配置されている。無線通信は、第1のデバイスにおける測定メッセージの到達時刻に基づいて第1のデバイスと第2のデバイスとの間の距離を測定するための測距プロトコルを含み、プロトコルは、第2のデバイスによって測定メッセージを送信することを含む。第1のデバイスは、第1のデバイスにおける測定メッセージの第1の到達時刻に基づいて第1のデバイスと第2のデバイスとの間の第1の距離を得るように構成されている。方法は、

協働デバイスにおける測定メッセージの第3の到達時刻を決定するステップと、

第3の到達時刻に基づくサポートデータを提供するステップと

を有する。第1のデバイスは、決定された距離を評価するために、サポートデータを使用して協働デバイスと第2のデバイスとの間の第3の距離を得ることと、第1の距離、信用される距離及び第3の距離に関する検証テストを実施することであって、検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する、検証テストを実施することとを行うように構成されている。

【0016】

上記の特徴には、第2のデバイスが測距プロトコルに参加するときに、第1のデバイスが、第2のデバイスによって送信されているものとしての測定メッセージの第1の到達時刻に基づいて、測距プロトコルに従って距離を決定するという効果がある。加えて、第3のデバイスが、第3のデバイスにおける同じ測定メッセージの第3の到達時刻を決定する。第3のデバイスは、第1のデバイスから距離において配置され、この距離は、第1のデバイスに知られており、信頼可能であるとして信用を得ている。そのような距離は、本明細書において信用される距離と呼ばれる。信用される距離は、予め決定されたか、又は、別個に測定され、若しくは、ユーザによって入力される。そのような第3のデバイスは、本明細書において協働デバイスと呼ばれる。

【0017】

協働デバイスとして動作する第3のデバイスは、何らかのさらなる測定メッセージを使用した測距プロトコルによるさらなる距離測定を実施しないことに留意されたい。代わりに、第3のデバイスは、協働して、第3のデバイスにおける上記同じ測定メッセージの第3の到達時刻を決定し、サポートデータを第1のデバイスに転送し、サポートデータは、第3の到達時刻に基づく。例えば、サポートデータは、基準クロック若しくはタイミンググリッドに対する、又は、同じく第1のデバイスによって受信される何らかの他のメッセージに対する第3の到達時刻データを含む。代替的に又は付加的に、サポートデータは、第3の距離データを含み、第3のデバイスは、さらなる受信メッセージ及び信用される距離を使用することによって、第3のデバイスと第2のデバイスとの間の第3の距離を決定することが可能である。

【0018】

サポートデータの受信を受けて、プロセッサが、サポートデータを使用して第3のデバイスと第2のデバイスとの間の第3の距離を得ることを可能にされる。その後、第1の距

10

20

30

40

50

離、信用される距離及び第3の距離に関する検証テストが実施される。有利には、検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する。

【0019】

一実施形態において、検証テストは、有効な空間的配置に関する余弦法則チェック又は三角不等式チェックを含む。有利には、チェックは、三角形の空間的配置が辺のそれぞれの長さを有するか否かを証明する。

【0020】

一実施形態において、測距プロトコルは、鍵データに基づいて暗号によって保護されているメッセージを交換することを含み、第1のメッセージプロセッサは、第3のメッセージプロセッサが、測距プロトコルに従ってメッセージを暗号論的に処理することを可能にするために、協働デバイスと鍵データを共有するように構成されている。有利には、第1のデバイスと第3のデバイスとの間のメッセージを暗号化することによって、そのようなメッセージが、悪意のあるものである可能性がある第2のデバイスによって改ざんされないように保護する。

【0021】

一実施形態において、第1のメッセージプロセッサは、測距プロトコルに従って信用される距離を決定するように構成されている。有利には、第2のデバイスに対する実際の測定に先立って、信用される距離が、同じ又は別の測距プロトコルを使用して決定される。

【0022】

一実施形態において、デバイスは、上記到達時刻を決定するための時間基準を提供するためのクロックユニットを備え、第1のメッセージプロセッサは、時間基準を、協働デバイス内の対応するクロックユニットと同期させるように構成されている。有利には、時間基準は、第1のデバイスと第3のデバイスとの間で共有される。第3の到達時刻は、時間基準に対して決定され、これは、サポートデータが、そのように決定された第3の到達時刻を含むことを可能にし、したがって、第1のデバイスによって使用可能である。

【0023】

一実施形態において、測距プロトコルは、第1のデバイスが、開始デバイスとして動作し、第2のデバイスに開始メッセージを送信することを含み、一方、開始メッセージが受信されると、第2のデバイスは、測定メッセージを送信する必要がある。第1のメッセージプロセッサは、第3のデバイスが距離測定のために開始デバイスとして動作することを可能にするために、第3のデバイスと役割変更データを交換するように構成されている。第3のデバイスは、役割変更データを受信すると、

第2の測定メッセージに基づいて測距プロトコルに従って第3のデバイスと第2のデバイスとの間の第3の距離を得ることと、

第3の方向を示す、第3のサポートデータを第1のデバイスに転送することを行うように構成されている。第1のメッセージプロセッサは、

第1のデバイスにおいて第2の測定メッセージを受信するときの第1のデバイスと第2のデバイスとの間の第2の距離を決定することと、

第3のデバイスから第3のサポートデータを受信することと、

第2の距離及び第3のサポートデータも使用して検証テストを実施することとを行うように構成されている。有利には、上記第2の距離を決定し、両方の距離を組み合わせることで検証することによって、第2のデバイスが、両方の距離測定値を一貫して改ざんすることがより困難になる。

【0024】

一実施形態において、第3のメッセージプロセッサは、第2のデバイスから受信される少なくとも1つのメッセージの第3の信号強度を決定し、第3の信号強度データを、第1のデバイスへのサポートデータに含めるように構成されている。第1のメッセージプロセッサは、第2のデバイスから受信される少なくとも1つのメッセージの第1の信号強度を決定し、第1の信号強度及び第3の信号強度を、決定された距離におけるそれぞれの予測

10

20

30

40

50

信号強度と比較することによって、決定された距離が信頼可能であるか否かを検証するように構成されている。任意選択的に、第1のデバイスと第3のデバイスの両方が、第2のデバイスからの同じメッセージの信号強度を測定する。有利には、決定された距離の検証を可能にする、さらなる独立したメカニズムが追加される。

【0025】

一実施形態において、第1のメッセージプロセッサは、決定された距離が信頼可能でないという評価を受けて、第2のデバイスに対する異なるセキュリティプロトコルを実行することを要求するように構成されている。有利には、代替的に又は付加的に、第1のメッセージプロセッサは、決定された距離が信頼可能でないという評価を受けて、異なる測距プロトコル及び／又は異なるタイプの無線通信を使用したさらなる距離測定を要求するように構成されている。代替的に、又は付加的に、第1のメッセージプロセッサは、決定された距離が信頼可能でないという評価を受けて、第1のデバイス内の少なくともいくつかのデータ及び／又は少なくとも1つの機能に対するアクセスを拒否又は制限するように構成されている。有利には、第1のデバイス内の任意の機能又はデータに対する悪意のあるアクセス又は使用が妨げられる。

【0026】

本発明のさらなる態様によれば、信頼可能な距離測定のためのシステムは、上述したようなデバイス及び第3のデバイスと、第1のデバイスから第2の信用される距離において配置されており、第3のデバイスから第3の信用される距離において配置されている、第2の協働デバイスとして動作する第4のデバイスとを備える。第4のデバイスは、メッセージを受信するための第4の無線レシーバと、

第4のメッセージプロセッサであって、第4のデバイスにおける測定メッセージの第4の到達時刻を決定することと、第4の到達時刻に基づく第4のサポートデータを第1のデバイスに転送することとを行うように構成されている、第4のメッセージプロセッサとを備える。第1のメッセージプロセッサは、第2の協働デバイスから第4のサポートデータを受信することと、第4のサポートデータを使用して第4のデバイスと第2のデバイスとの間の第4の距離を得ることと、第2の信用される距離及び第4の距離も使用して検証テストを実施することとを行うように構成されている。有利には、上記さらなる距離を決定し、すべての距離を組み合わせて検証することによって、第2のデバイスが、上記距離を一貫して操作することがより困難になる。

【0027】

任意選択的に、検証テストは、少なくとも2つの空間的配置に関する三角不等式の組み合わせを使用し、各配置は、第2のデバイスと、第1のデバイス及び協働デバイスのセットのうちの2つのデバイスとを含む。任意選択的に、第1のメッセージプロセッサは、第1の空間的配置による第2のデバイスの第1の位置が第2の空間的配置による第2のデバイスの第2の位置に対応するか否かを検証するように構成される。

【0028】

任意選択的に、第1のメッセージプロセッサは、決定された距離のすべてがゼロよりも大きいかな否かを決定するための非一貫性チェックを使用して検証テストを実施するように構成される。

【0029】

任意選択的に、第1のメッセージプロセッサは、第3のデバイスから第1のデバイスへの線と、第4のデバイスから第1のデバイスへの線との間の信頼できる角度が少なくとも90度になるように、第3のデバイス及び第4のデバイスが配置される構成に基づいて検証テストを実施するように構成される。

【0030】

任意選択的に、第1のメッセージプロセッサは、第3のデバイス及び第4のデバイスが第1のデバイスに関して互いに対向して配置される構成に基づいて検証テストを実施するように構成される。

【0031】

任意選択的に、第1のメッセージプロセッサは、第2の信用される距離が信用される距離に対応する構成に基づいて検証テストを実施するように構成される。

【0032】

一実施形態において、システムは、さらなる協働デバイスとして動作する少なくとも1つのさらなるデバイスを備え、第3のデバイス、第4のデバイス及び少なくとも1つのさらなるデバイスは、一平面内で、多角形のエッジに配置され、第1のデバイスは多角形の内部にあり、第1のメッセージプロセッサは、

少なくとも2つの空間的配置に関する三角不等式の組み合わせを使用して検証テストを実施するように構成されており、各配置は、第2のデバイスと、第1のデバイス及び協働デバイスのセットのうちの2つのデバイスとを含む。有利には、上記さらなる距離を決定し、すべての距離を組み合わせで検証することによって、第2のデバイスが、上記距離を一貫して操作することがより困難になる。

【0033】

一実施形態において、方法は、第1のデバイスに、第1の到達時刻又は第1の距離を提供するための開始デバイスとして動作するように命令するステップを有する。代替的に、又は付加的に、方法は、第3のデバイスに、第3の到達時刻に基づくサポートデータを提供するための協働デバイスとして動作するように命令するステップを有する。実効的に、ここで、距離測定の制御は、上記命令によって実施される。

【0034】

上記において、明確にするために、第1のデバイスが、距離測定及び距離信頼性検証を実施すると記載されていることに留意されたい。しかしながら、第1のデバイス、第3のデバイス及び／又はさらなる協働デバイスが、すべての必要な情報を、距離測定及び距離信頼性検証を実施する制御デバイスに提供することも可能である。

【0035】

本発明による方法は、コンピュータ実施方法としてコンピュータ上で実施され、又は、専用ハードウェア内で実施され、又は、その両方の組み合わせである。本発明による方法の実行可能コードは、コンピュータプログラム製品上に記憶される。コンピュータプログラム製品の例は、メモリスティックなどのメモリデバイス、光ディスクなどの光学記憶デバイス、集積回路、サーバ、オンラインソフトウェアなどを含む。コンピュータプログラム製品は、上記プログラム製品がコンピュータ上で実行されるときに、本発明による方法を実施するための、コンピュータ可読媒体上に記憶されている非一時的プログラムコード手段を含む。一実施形態において、コンピュータプログラムは、コンピュータプログラムがコンピュータ上で作動されているときに、本発明による方法のすべてのステップ又は段階を実行するようになされたコンピュータプログラムコード手段を含む。コンピュータプログラムはコンピュータ可読媒体上に具現化されることが好ましい。ネットワークからダウンロード可能であり、並びに／又は、コンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶されるコンピュータプログラム製品が提供され、製品は、コンピュータ上で実行されるときに、上述したような方法を実施するためのプログラムコード命令を含む。

【0036】

本発明の別の態様は、例えば、位置に基づくアプリケーションに含まれる、ダウンロードに利用可能なコンピュータプログラムを作製する方法を提供する。この態様は、コンピュータプログラムが、例えば、AppleのApp Store、GoogleのPlay Store、又はMicrosoftのWindows Storeにアップロードされるときに、及び、コンピュータプログラムがそのようなストアからダウンロードのために利用可能であるときに、使用される。

【0037】

本発明によるデバイス及び方法のさらなる好ましい実施形態が、添付の特許請求の範囲において与えられ、その開示は参照により本明細書に組み込まれる。

【0038】

本発明のこれらの及び他の態様は、例として以下の説明に記載されている実施形態から明らかになり、さらにそれらの実施形態及び添付の図面を参照することによって明らかにされる。

【図面の簡単な説明】

【0039】

【図1】無線通信及び距離測定のためのデバイスを示す図である。

【図2】無線通信のためのデバイス及び協働デバイスの空間的配置を示す図である。

【図3】無線通信のための2つのデバイスの空間的配置を示す図である。

【図4】無線通信のための2つのデバイスのさらなる空間的配置を示す図である。

【図5】2つの協働デバイスを有する空間的配置を示す図である。

【図6】2つの協働デバイスを有する第2の空間的配置を示す図である。

【図7】2つの協働デバイスを有するさらなる空間的配置を示す図である。

【図8】距離測定のための方法を示す図である。

【図9】距離測定において協働デバイスとして動作するための方法を示す図である。

【図10a】コンピュータ可読媒体を示す図である。

【図10b】プロセッサシステムの概略図である。

【発明を実施するための形態】

【0040】

図面は純粋に図式的なものであり、原寸に比例して描かれたものではない。図面において、すでに記載されている要素に対応する要素は、同じ参照符号を有する。

【0041】

後述するような無線通信を使用した距離測定は、少なくとも基本的な機能を提供する、すなわち、例えば、固定位置にあるモバイルデバイスと別のデバイスとの間の現在の位置に関する情報を提供する。以降説明される実施形態を使用して増強される、測定メッセージの到達時刻を使用した適切な測距プロトコルの例として、様々なプロトコルがここで説明される。

【0042】

距離測定の第1の例が、[802.11]に記載されている。clause 11.24.6は、ファインタイミング測定（FTM）手順を規定している。FTMメカニズムは、RF波が光速で一方のデバイスから他方のデバイスへと進行するのにかかる時間を補償することもできるように、2つのデバイス内のクロック間の絶対時間の差を測定するように意図されている。FTM手順において、デバイスの一方は、他方のデバイスが2つのデバイスの間の往復時間（RTT）を測定することができるように（後に説明する）、そのクロックのタイムスタンプを送信する。802.11（Wi-Fi（登録商標））を使用した2つのデバイス間の距離測定は、[802.11]のclause 11.24.6に指定されているファインタイミング測定（FTM）手順を使用して往復時間（RTT）を測定し、RTTに光速を乗算し、2で除算することによって行うことができる。

【0043】

以下は、[802.11]におけるFTMの説明である。例えば、図11-35、図11-36、図11-37及び周囲のテキストを参照されたい。下記のタイムスタンプのナンバリングは、図11-36からのものである。開始STA（ステーション）が、別のSTA、応答STAまでのRTT又は距離を知りたいことを所望する。これを達成するために、開始STAは、初期FTM要求を応答STAに送信する。応答STAは、FTM__1（0，0）メッセージを開始STAに送信し、正確な送信時刻を測定する。応答STAは、この時刻を t_{1_1} として記憶する。開始STAは、FTM__1（0，0）メッセージの受信を t_{2_1} として測定する。これは、結果としてのACKの送信時刻を t_{3_1} として測定する。しかしながら、開始STAは、値 t_{2_1} 及び t_{3_1} を直ちに使用することはできない。

【0044】

応答STAは、FTM__1（0，0）への応答として受信されるACKの受信時刻を測

定し、これを t_{4_1} として記憶する。しばらく（少なくとも $Min\ Delta\ FTM$ 秒）後、応答 STA は、 FTM_2 (t_{1_1} , t_{4_1}) を送信し、送信時刻を t_{1_2} として記録する。この開始 STA は、上述したものと同一ルーティンを踏む、すなわち、 FTM_2 (t_{1_1} , t_{4_1}) の受信時刻を t_{2_2} として測定し、 ACK の送信時刻を t_{3_2} として測定する。しかしながら、今回、開始 STA は、 $[802.11]$ からの以下の式 (11-5) に従って RTT を測定することが可能である。

$$RTT = [(t_{4_1} - t_{1_1}) - (t_{3_1} - t_{2_1})] \quad (1)$$

上記式の右辺を再整理すると、以下のようになる。

$$RTT = (t_{2_1} - t_{1_1}) + (t_{4_1} - t_{3_1}) \quad (2)$$

ここから、 $(t_{2_1} - t_{1_1})$ が、 FTM フレームを転送している間に FTM フレームが RF 媒体にわたって応答 STA から開始 STA へと進行するための時間であり、 $(t_{4_1} - t_{3_1})$ が、 ACK フレームが RF 媒体にわたって開始 STA から応答 STA へと進行するための時間であり、結果、それらの合計が実際の往復時間であることが容易に分かる。

【0045】

正確度を増大させるために、上記を繰り返すことができ、 RTT は、すべての測定値の平均として計算することができる。

【0046】

t_{1_X} は出発時刻である。 TOD は、 $[802.11]$ において、「 TOD [...] は、時間基準に対する、最後に送信されたファインタイミング測定フレームのプリアンプルの始まりが送信アンテナコネクタに現れた時刻を表す」として定義されている。プリアンプルは、 PHY フレームの本当に最初の部分であり、これは、とりわけ、トランスミッタがプリアンプルの直前に一切の RF エネルギーを伝送しないことを意味する。その後、開始 STA は、同じように t_{3_X} を測定しなければならない、すなわち、 t_{3_X} は、時間基準に対する、受信ファインタイミング測定フレームへの応答としての、最後に送信された ACK フレームのプリアンプルの始まりが送信アンテナコネクタに現れた時刻を表す。

【0047】

t_{4_X} は到達時刻である。 TOA は、 $[802.11]$ において、「 TOA [...] は、時間基準に対する、最後に送信されたファインタイミング測定フレームに対する ACK フレームのプリアンプルの始まりが送信アンテナコネクタに到達した時刻を表す」として定義されている。その後、開始 STA は、同じように t_{2_X} を測定しなければならない、すなわち、 t_{2_X} は、時間基準に対する、最後に受信されたファインタイミング測定フレームのプリアンプルの始まりが受信アンテナコネクタに到達した時刻を表す。

【0048】

したがって、最小時間 $t_3 - t_2$ は、受信 FTM (,) フレーム + $SIFS$ の長さに等しく、最大時間 $t_3 - t_2$ は、受信 FTM (,) フレーム + $DIFS$ の長さに等しい。 FTM (,) フレームの長さは変動する。本明細書の残りの部分において、以下の定義を使用する。

t_2 及び t_3 を測定するために開始 STA においてもたらされた物理 FTM フレームの時間長を示すために L_{ftm} を使用する。

応答時間、又は開始 STA の応答時間という用語及び記号 R を、開始 STA が、物理 FTM フレームの最後のシンボル（すなわち、 CRC チェックの最後のシンボル）がその受信アンテナコネクタに到達した直後から、 FTM フレームに応答して送信した ACK フレームの TOD までにかかる時間として使用する。 ACK フレームの送信は割に単純な動作であるため、これはハードウェアにおいて行われる可能性が高く、したがって、一定である。

【0049】

$[802.11]$ の $clause\ 11.24.6$ は、タイミング測定 (TM) 手順を指定している。 FTM 手順からのいくつかの差異があり、最も注目すべき差異は、タイムスタンプの分解能がより良好であることであり、これは原則的に、より精密な距離測定を可

10

20

30

40

50

能にする。下記の実施形態は、T Mに対して、F T Mについて本明細書に記載されているのと同じように使用される。

【0050】

F T Mに類似した距離測定システムのさらなる例が、米国特許第8762727号明細書に記載されている。その差異は、開始S T Aがソースノードと呼ばれること、応答S T Aがターゲットノードと呼ばれること、並びに、ソースノードがt 1及びt 4を測定し、ターゲットノードがt 2及びt 3を測定し、これらをソースノードに送信することである。

【0051】

距離測定システムは、距離測定システムのさらなる例が、3 G P Pに記載されており、これはO T D O A（観測到達時刻差）と呼ばれる。[O T D O A]を参照されたい。これは、r e l 9 E－U T R A（L T Eラジオ）に導入されている位置決め機能である。下記に明らかにされているような参考文献[36. n n n]を参照されたい。これは、ユーザ機器（U E）が、いくつかのe N o d e B（すなわち、基地局）からのいくつかの特定の信号、すなわち、位置決め基準信号P R S間の時間差を測定し、これらの時間差をネットワーク内の特定のデバイス、すなわち、位置サーバ（進化型サービングモバイルロケーションセンタE－S M L C）に報告するマルチラレーション方法である。これらの時間差及びe N o d e Bの知識に基づいて、E－S M L CはU Eの位置を計算する。L P P（L T E測位プロトコル）の記述は、[36. 355]仕様書に見出すことができる。P R S信号の正確な詳細は[36. 211]のs e c t i o n 6. 10. 4に見出すことができ単純なO T D O A手順は、[37. 571-1]仕様書のs e c t i o n 9のR A N 5 O T D O A試験事例の記述に見出すことができる。W i - F i（登録商標）における位置特定に関する測定とまったく同様に、モバイルデバイスは、これらのO T D O Aレポートを、モバイルデバイスが所望するとこのネットワークにも現れるように偽装することができる。これらの下記の実施形態は、このタイプの不正行為に対して保護するために使用される。同じ測定がO T D O AにおいてU Eによって行われるための別の用語は、R S T D（基準信号時間差）である。R S T D測定正確度要件は、[36. 133]に規定されている。

【0052】

3 G P Pにおける距離測定のさらなる例は、タイムグリッドに対するメッセージの到達時刻に基づき、高位化セルI Dベース又はE－C I Dと呼ばれる。セルI Dベースの方法は、r e l 9以前にすでに可能であった。高位化セルI Dは、いくつかのすでに利用可能な測定値とともに集約し、それらのいくつかは、位置決め正確度機能を改善するために正確度要件が増大されている。高位化セルI D、E－C e l l I D、又はE－C I Dは、r e l 9 E－U T R A（L T Eラジオ）に導入されている位置決め機能である。U Eはネットワークに（サービングセル又はe N o d e Bを通じて位置測定サーバ、すなわち進化型サービングモバイルロケーションセンタE－S M L Cに）サービングセルI D、サービングセルによるタイミングアドバンス（その送信時刻と受信時刻との間の差）、基準（狭帯域）信号受信電力（R S R P／N R S R P）、（狭帯域）基準信号受信品質（R S R Q／R S R Q）を報告する。R S R P／N R S R P及びR S R Q／R S R Qは、任意の隣接するセルから測定及び報告され、一方、タイミングアドバンスは、プライマリセル（サービングセル）のみについて測定される。サービングセル又はe N o d e Bは、到達角度のような追加の情報をE S M L Cに報告する。E S M L Cは、この情報及びセル位置のその知識に基づいてU E位置を推定する。

【0053】

タイミングアドバンスの測定は以下の通りである。L T E又はG S Mにおいて、セルが、固定タイミングを有する送信又は受信機会の周波数－時間グリッドを送信する。L T Eについて、個々の周波数は、O F D Mサブキャリアの周波数であり、通常、15 k H z 離れている。時間ドメインは、10 m sの連続するフレームから成り、各フレームは10個のサブフレームから成り、各サブフレームは0.5 m sの2つのスロットから成る。この周波数－時間グリッドは、セルによって非常に厳密なタイミングによって維持される。グ

10

20

30

40

50

リッド要素ごとに、セルは、範囲内のすべてのモバイルデバイスに（ブロードキャスト）又は1つの特定のデバイスに送信していることができる。グリッド要素（周波数、サブフレーム組み合わせ又は時として周波数とスロットとの組み合わせ）の一部において、セルは、3 G P P仕様において定義されているものとしては、常に送信していることになる。したがって、これらのグリッド要素は理想的には、柔軟に使用することができるグリッド要素の各々の目的などのシステム情報を、セル内のモバイルデバイスに送信するのに適している。そのため、他のグリッド要素、すなわち、より柔軟に使用することができる要素の各々において、セルは、範囲内のすべてのモバイルデバイスにブロードキャストしているか、特定のモバイルデバイスに送信しているか、又は、特定のモバイルデバイスに、セルに若しくはセル内の別のモバイルデバイスに送信する許可を与えている。

10

【0054】

R F波がセルからモバイルデバイスへと進行するには時間がかかるため（約300メートル毎マイクロ秒）、グリッドは、モバイルデバイスには、この進行時間だけ遅延されているように見える。この進行時間を τ 秒と仮定する。モバイルデバイスが送信を許可されているサブフレームの始まりから正確に送信を開始するとき、モバイルデバイスは、セルにおけるサブフレームの始まりよりも τ 秒遅く送信を開始する。モバイルデバイスによって送信されている信号がセルに到達するにも τ 秒かかる。それゆえ、セルがモバイルデバイスからの送信を受信するのは、正確に、それに割り当てられているサブフレームの始まりにおいてではなく、 2τ 秒遅い。この遅延を測定することによって、セルは、モバイルデバイスまでの距離を決定することができる。

20

【0055】

モバイルデバイスがセルから遠く離れている場合、あるサブフレーム内のその送信の終わりは、次のサブフレームの始まりよりも遅くなり、そのため、干渉が起こる。この問題を克服するために、セルは、モバイルデバイスに、その特定のモバイルデバイスにアドレス指定されたタイミングアドバンスコマンド内のいわゆるT A値にコード化されている一定量のタイミングアドバンスを使用するように求めることができる。このとき、モバイルデバイスは、モバイルデバイスによって決定するものとしてのサブフレームの始まりよりも早く、その送信T Aを開始する。タイミングアドバンスに可能な最大値は0.67msであり、これは、100kmよりもわずかに長い、モバイルデバイスーセル距離に対応する。技術仕様書3 G P P T S 36.321 [36.321]、section 6.1.3.5「タイミングアドバンスコマンドM A C制御要素」は、L T EのT A値調製手順を記載している。

30

【0056】

異なる距離に現れることを所望するモバイルデバイスは、セルのより近くに現れることを所望するときは周波数－時間グリッド若しくは送信セルから受信したT A値だけ、仮定されているよりも早くその送信を開始するか、又は、現実にはそうであるよりもセルから遠くに現れることを所望するときは、仮定されているよりも遅く送信を開始することができる。

【0057】

正確且つ正しい距離測定が、いくつかの用途において重要である。例えば、W i - F i（登録商標）によって自動車からキー FOBまでの距離を測定するためにW i - F i（登録商標） F T Mが使用され、そのため、自動車が、測定距離が例えば5メートル未満であるときにそのドアを開くことを決定することができるとき、キー FOBまでの実際の距離は、実際には5メートル未満であるということが重要である。別の例は、他のデバイスが特定のデバイスから離れていない場合に、デバイスが、著作権のあるコンテンツのみを別のデバイスにストリーミングすることを許可されるということである。正確且つ正しい距離測定を使用して、セキュアな認証されたチャネルを構成するときに中間者攻撃を防止することもできる。これは次の段落で説明する。

40

【0058】

2つのデバイスは、それらの有線又は無線通信の安全を確保する必要がある場合、それ

50

らの通信を暗号化する。しかしながら、これは、両方の無線デバイスが同じ鍵を知っていることを必要とする。ディフィー・ヘルマン [DH] は、2 者の当事者間で秘密鍵を確立するよく知られた技法であり、秘密鍵を確立するための当事者間の通信は、確立される秘密鍵に関する一切の情報を第三者に明かさない。2 者の当事者は各々、自身の公開／秘密鍵対を使用し、公開鍵を互いに交換する。各当事者は、自身の秘密鍵及び他方の当事者の公開鍵、並びに、場合によっては、各当事者からの、例えばノンス（乱数）などの何らかの他の情報を使用して秘密鍵を計算することが可能である。各当事者は、ディフィー・ヘルマンを実施する度に、又は、古い鍵対を再使用する度に、新たに鍵対を生成する。

【0059】

ネットワークを介してディフィー・ヘルマンを実施するとき、ディフィー・ヘルマンを実施するための公開鍵を受信するデバイスは、この公開鍵がいずれのデバイスからのものであるかを知らない。このことが、いわゆる中間者攻撃において攻撃者によって利用される。攻撃者 E は、デバイス A が接続を所望する現実のデバイス B になりすまし得る。攻撃者 E は、デバイス A とディフィー・ヘルマンを実施し、デバイス A との秘密鍵 K_{ae} を確立する。同様に、攻撃者は、デバイス B に対してデバイス A になりすまし、デバイス B との秘密鍵 K_{be} を確立する。デバイス A 又は B のうち的一方からのメッセージが入来すると、攻撃者は、一方の秘密鍵を用いてメッセージを解読し、他方によってこれを暗号化し、これを他方のデバイスに転送する。このように、デバイス A 及び B は、いくらかの遅延が加わることを除いて、それらの通信において不審な点に一切気付かない。それらのデバイスが、別の通信方式を使用して同じ情報を送信し、結果を比較することによってそれらの通信をチェックするとき、それらのデバイスは、それらの通信に伴う一切の改ざんに気付かない。しかし、攻撃者は、それらのデバイスが通信する内容に関する完全な知識を有する。

【0060】

デバイスプロビジョニングプロトコル [DPP] において、第 1 のステップは、DPP ブートストラッピング、すなわち、他方のデバイスの、中間者デバイスの公開鍵ではない公開ブートストラッピング鍵において信用を得るための手順を実施することである。ブートストラッピング方法のうちの一つは、他方のデバイスによる表示又は他方のデバイス上の印刷としての、他方のデバイスの公開ブートストラッピング鍵を含む QR コード（登録商標）を走査することである。他方のデバイスもまた、第 1 のデバイスの QR コード（登録商標）を走査する（相互認証）。その後、ブートストラッピング鍵が DPP 認証プロトコルにおいて使用され、他方のデバイスが公開ブートストラッピング鍵に属する秘密鍵をも保持するか否かがチェックされる。DPP における公開ブートストラッピング鍵が Wi-Fi（登録商標）（例えば、近接認識ネットワークング [NAN] など、任意の形態の Wi-Fi（登録商標））を介して交換されている場合、それらは、RF 範囲内のいかなるデバイスによっても送信されている可能性があるため、信用することができない。引き続き DPP について、DPP 認証プロトコルは、共通の共有鍵 K_e の確立をもたらすが、デバイスには、それらがこの鍵を意図したデバイスと共有しているか、又は、中間者デバイスと共有しているかは分からない。同様に、日と見無線暗号化 [OWE] を使用するとき、公開鍵は、Wi-Fi（登録商標）を介して、ディフィー・ヘルマンを使用することによって交換され、共通の共有鍵が、2 つのデバイスの間の後続の通信の暗号化のために確立される。

【0061】

一方、中間者デバイスとの共通の共有鍵が構成される確率を制限するための方策は、デバイスが他のデバイスまでの距離を測定し、この距離が、例えば数メートルなど、デバイス内の規則によって又はそのユーザによって決定されるような特定の距離未満である場合、それらのデバイスは他のデバイスから受信される公開鍵を信用するというものである。ユーザはこの場合、Wi-Fi（登録商標）を介して公開鍵を送信したデバイス、そのため、意図されたデバイス又は中間者デバイスが離れている距離が距離制限未満であることを知る。その後、ユーザは、この範囲内に意図されるもの以外の何らかの他のデバイスが

存在するか否かを判定することができる。

【0062】

距離測定を使用して中間者デバイスとの共通の共有鍵が構成される確率を制限することは、最初にWi-Fi（登録商標）を介して公開鍵を交換し、次いで、例えば、OWE又はDPPのDPP認証プロトコル部分（DPPブートストラッピングがWi-Fi（登録商標）、例えばWi-Fi（登録商標） Awareを介して行われる）によって共有セッション鍵を計算し、その後、日和見無線暗号化[OWE]、DPP若しくは何らかの他の方法によって、又は、少なくとも、FTM__Xフレーム内の t_1 及び t_4 値を含むフィールドを暗号化することによって、決定される共有セッション鍵を使用して暗号化FTM__Xフレームを使用するFTM手順を実行することによって行うことができる。要求STAまでのそのように測定された距離がxメートル未満である場合、開始STAは受信された公開鍵を信用することができ、合意されたセッション鍵を使用して他のデバイスとのさらなる通信に進むことができる。DPPの場合、さらなる通信はDPP構成プロトコルである。OWEの場合、これは、APとSTAとの間の暗号化WAN接続である。開始STAはまた、応答STAまで測定される距離内にWi-Fi（登録商標）デバイスが1つしかないと確信しているか否かを尋ねることもでき、ユーザがこれを確認した場合、開始STAは共有セッション鍵の使用を進める。

【0063】

上記で説明したように、応答STAは、開始STAが、現実にそうであるのとは別の距離にあると考えるようにする理由を有する。特に、応答STAは、 t_4 __X値を低減すること及び／又は t_1 __X値を増大させることによって、開始STAが、現実にそうであるよりも近いと考えるようにすることができる。これは、[802.11]の式(11-5)から容易に理解される。

$$RTT = [(t_4_X - t_1_X) - (t_3_X - t_2_X)] \quad (3)$$

2つのデバイス間の距離は以下のとおりである。

$$d = c * RTT / 2 \quad (4)$$

ここで、cは光速（約 $3 * 10^8 \text{ m/s}$ ）である。

【0064】

開始STAによって測定されるものとしての距離を1メートル低減するためには、応答STAは、 t_4 __Z及び t_1 __Xの差を、それらの測定値から以下の値だけ低減する必要がある。

$$\Delta t = 2 * 1 \text{ m} / 3 * 10^8 \text{ m/s} = 2 * 3.33 * 10^{-9} \text{ s} = 6.66 \text{ ns} \quad (5)$$

しかしながら、応答STAは、 t_4 __X及び t_1 __Xの差を開始STAに報告するときに、それらの差をそれらの測定値から低減しすぎないように注意する必要がある。これは、このとき、開始STAが負のRTTを測定することになるためである。報告されている t_4 __Z及び t_1 __Xの差が開始STAの応答時間、すなわち、 t_3 __Xと t_2 __Xとの間の差に等しいとき、開始STAは0の往復時間を測定することになる。したがって、不正行為に成功するには、応答STAが開始STAの t_3 __X及び t_2 __Xの差を知っていることが重要である。

【0065】

上記で説明したように、開始STAの t_3 __X及び t_2 __Xの差は2つの部分、すなわち、FTM PHYフレームの長さ(L f t m)及び応答時間Rから成る。応答STAはFTMフレーム自体を送信しており、そのため、その時間長L f t mを知っている。応答時間Rは、様々な状態で応答STAに知られる。

不正デバイスが何らかの方策によって開始STAまでの現実の距離を知っており、したがって、報告される t_1 及び t_4 を適合させることによって、開始STAが測定する距離を精密に偽装することができると仮定する。そのため、上述したようなFTMを使用した測定を行うことによる問題は、悪意のある応答STAが、現実にそうであるよりも開始STAに対して近く又は遠くにあるように見えるように、その報告される到達時刻 t_1 及び

t 4 を操作することができることである。

【0066】

距離の偽装に成功するのを防止するために、開始デバイスは、開始デバイスに対して既知の位置にある1つ又は複数の協働デバイスを伴う。協働デバイスは、開始デバイスのクロックと同期されたクロックを利用し、又は、何らかの他の時間基準を共有する。協働デバイスは、測定メッセージの到達時刻を独立して測定し、これらを開始デバイスに報告する。開始デバイスは、不正な応答デバイスによる操作された到達時刻測定を審理及び検出するために、三角形からの特性を使用する。3 G P P に基づくシステムについて、開始デバイス及び1つ又は複数の協働デバイスは、基地局によって具現化され、応答デバイスは、ユーザ機器 U E によって具現化される。

10

【0067】

距離に基づく測定をより信頼可能に行うことによって、これは、信頼可能な近接性に基づくサービスにとって有効なツールになる。いくつかの例示的な使用事例は、以下を含む。

－近傍の無線キーボード、近傍の無線記憶デバイス、近傍のセンサ又は近傍の無線ウェブカメラに接続する場合に、正しいものに接続し、行われていることを監視、コピー又は追跡することを所望する何らかの中間者デバイスには接続しないことを保証することを所望する。

－友人に会い、友人の携帯電話に接続して何らかの写真を交換することを所望する場合に、中間者ではなく、友人の携帯電話に接続することを保証することを所望する。

－家屋又は店の中で何らかのデバイスを自動的にオンにすること、何らかの扉を開くこと、又は、人が近接近しているときにそのモバイルデバイスを用いて何らかのサービスに接続することを可能にすることを所望する場合に、そのモバイルデバイスの位置が正しく、近くにあることを主張する偽りのデバイスではないことを保証することを所望する。

20

－店内で取引を開始することを所望する場合、例えば、レジに近いとき、フィッシング攻撃を受けており、それによってユーザが、店によって提供される公式サービスの代わりに、遠く離れて位置するフィッシングデバイスに気付いておらず、接続しているということがないことを保証することを所望する。

【0068】

図1は、無線通信及び距離測定のためのデバイスを示す。無線通信のためのデバイスの空間的配置100は、第1のデバイス110及び第2のデバイス120を含み、これらのデバイスは距離151において物理的に離れている。第1のデバイスは、メッセージを送信及び受信するための第1のトランシーバ111と、第1のメッセージプロセッサ112とを有する。第2のデバイスは、無線レシーバ121、又は第2のトランシーバと、第2のメッセージプロセッサ122とを有する。また、第3のデバイスも、第3のトランシーバ131と、第3のメッセージプロセッサ132とを有する。これらのデバイスは、トランシーバ111、121、131に接続されているアンテナ113、123、133によって概略的に示されているように、無線通信に対応している。

30

【0069】

これらのデバイスは、下記にさらに説明するように、第1のデバイスと第2のデバイスとの間の距離を決定するための、第1のデバイスと第2のデバイスとの間の測距プロトコルによる、無線通信を介した距離測定のために構成されている。無線通信は、第1のデバイスにおける測定メッセージの到達時刻に基づいて第1のデバイスと第2のデバイスとの間の距離を決定するための測距プロトコルを含む。プロトコルは、第2のデバイスによる測定メッセージの送信を含む。これらの例において、無線通信及び測距プロトコルは[802.11]に従うが、到達時刻測定に基づいて適切な測距プロトコルを提供する、Bluetooth (登録商標)などの他の無線プロトコルも使用される。

40

【0070】

第1のメッセージプロセッサ112は、測距プロトコルに従ってメッセージを処理し、第1のデバイスにおける測定メッセージの第1の到達時刻を決定し、第1の到達時刻に基づいて第1のデバイスと第2のデバイスとの間の第1の距離151を決定するように構成

50

されている。加えて、第1のメッセージプロセッサは、第3のデバイス130と通信するように構成されている。第3のデバイスは、協働デバイスとして動作し、第1のデバイスから信用される距離150に位置する。信用される距離は、第1のデバイスに知られており、信頼可能であるとして信用を得ている。信用される距離は、予め決定されたか、又は、別個に測定され、若しくは、ユーザによって入力される。任意選択的に、第1のメッセージプロセッサは、第3のデバイスによって実行される測距プロトコルに従って信用される距離を決定するように構成されている。第2のデバイスに対する実際の測定に先立って、信用される距離が、同じ又は別の測距プロトコルを使用して決定される。

【0071】

協働デバイスとも呼ばれる第3のデバイスにおいて、第3のメッセージプロセッサ132は、第3のデバイスにおける測定メッセージの第3の到達時刻を決定するように構成されている。特に、第3のデバイスは、第3のデバイスにおける上記同じ測定メッセージの第3の到達時刻を決定し、サポートデータを第1のデバイスに転送することによって、第1のデバイスと協働し、サポートデータは、第3の到達時刻に基づく。例えば、サポートデータは、基準クロック若しくはタイミンググリッドに対する、又は、同じく第1のデバイスによって受信される何らかの他のメッセージに対する第3の到達時刻データを含む。代替的に又は付加的に、サポートデータは、第3の距離データを含む。それに加えて、第3のデバイスは、例えば、さらなる受信メッセージ及び信用される距離を使用することによって、第3のデバイスと第2のデバイスとの間の第3の距離を決定することが可能である。

【0072】

第1のメッセージプロセッサは、決定された距離の評価のために、協働デバイスからサポートデータを受信し、サポートデータを使用して第3のデバイスと第2のデバイスとの間の第3の距離153を得るように構成されている。第1のメッセージプロセッサは、その後、第1の距離151、信用される距離150及び第3の距離153に関する検証テストを実施するように構成されている。検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する。例えば、検証テストは、下記にさらに明らかにされるように、有効な空間的配置に関する余弦法則チェック又は三角不等式チェックを含む。チェックは、決定された距離に従って、三角形の現実の空間的配置がそれぞれの辺の長さを有するか否かを証明することを目的とする。

【0073】

測距プロトコルは、鍵データに基づいて暗号によって保護されているメッセージを交換することを含む。任意選択的に、第1のメッセージプロセッサは、第3のメッセージプロセッサが、測距プロトコルに従ってメッセージを暗号論的に処理することを可能にするために、協働デバイスと鍵データを共有するように構成されている。それ自体既知である無線通信プロトコルに従って第1のデバイスと第3のデバイスとの間のメッセージを暗号化することによって、そのようなメッセージが、悪意のあるものである可能性がある第2のデバイスによって改ざんされないように保護する。

【0074】

任意選択的に、デバイスは、上記到達時刻を決定するための時間基準を提供するためのクロックユニットを有する。第1のメッセージプロセッサは、時間基準を、例えば、[802.1AS]のプロトコルによって同期されている、協働デバイス内の対応するクロックユニットと同期させるように構成されている。有利には、時間基準は、第1のデバイスと第3のデバイスとの間で共有される。第3の到達時刻は、時間基準に対して決定され、これは、サポートデータが、そのように決定された第3の到達時刻を含むことを可能にし、したがって、第1のデバイスによって使用可能である。

【0075】

以下において、1つ又は複数の協働STAが加わることは、応答STAが、現実にもそうであるよりも開始STAのより近くにあるように見えることを所望することを検出するこ

10

20

30

40

50

とを、どのように及びどの程度助けることができるかが記載されている。以下の仮定が適用される。

応答 S T A は、開始 S T A に対して任意の距離にあるように見えるように、自身が開始 S T A に報告する測定値をどのように調整するかを知っている。

開始 S T A 及び協働 S T A は、802.1AS プロトコル [802.1AS] と同期されている物理フレームの到達時刻及び出発時刻を計るクロックを有し、又は他の状態で、開始 S T A が、対応する S T A のいずれの測定値をそれ自体のいずれの測定値と組み合わせるべきか分かるように、通信する。

開始 S T A 及び協働 S T A は、協働 S T A に必要な情報を共有し、結果、協働 S T A は、応答 S T A からの F T M (,) メッセージを受信、識別、及び必要に応じて解釈することができ、そのため、協働 S T A は、応答 S T A からの F T M (,) メッセージの到達時刻を測定し、これらを開始 S T A に報告することができ、結果、開始 S T A は、これらの到達時刻を、同じメッセージ上のそれ自体の測定値と組み合わせることができる。

F T M 測定は、2 回以上実施され、すべての S T A の測定及び報告されている時刻 t_1 、 t_2 、 t_3 及び t_4 は最初に平均され、その後、それらは距離及び位置の計算に使用され、結果、測定正確度は、信頼可能な結果を得るのに十分に良好になる。

【0076】

下記において、タイミング測定のみを行うことができる、S T A に対する強力な攻撃に対する良好な防衛が説明される。そのような防衛において、開始 S T A は 1 つ又は複数の協働 S T A と協働し、図示されているように三角不等式を適用し、協働 S T A が 2 つ以上ある場合は、計算されている位置において不一致のチェックを適用する。詳細な例は、[802.11] の F T M プロトコルを使用して与えられる。しかしながら、これは、1 つのデバイスがプロトコルメッセージの到達時刻、出発時刻、又はその差を別のデバイスに報告する、W i - F i (登録商標)、B l u e t o o t h (登録商標) 又は任意の他の無線 (また、光学も) 技術を使用する距離測定技術によって最良に機能する。

【0077】

図 2 は、無線通信のためのデバイス及び協働デバイスの空間的配置を示す。配置 200 は、開始 S T A と呼ばれる第 1 のデバイス 210 と、応答 S T A と呼ばれる第 2 のデバイス 220 と、協働 S T A と呼ばれる第 3 のデバイス 230 とを含み、これらのデバイスは図 1 を参照しながら説明したデバイスと同様である。第 1 の距離 d_1 $_c$ が、現実の距離 d_1 (又は d) にある第 1 のデバイス 210 と第 2 のデバイス 220 との間で決定される。第 3 の距離 d_2 $_c$ が、第 3 のデバイス 230 と第 2 のデバイス 220 との間で決定される。信用される距離 L が、現実の距離 d_2 にある、第 1 のデバイス 210 と第 3 のデバイス 230 との間にある。

【0078】

この例において、不正な応答 S T A から開始 S T A までの現実の距離は d であり、これは、不正な応答 S T A から協働 S T A までの距離でもある。開始 S T A は、上述した方法のいずれかをを用いて不正な応答 S T A までの距離測定を実施する。残りの部分においては、F T M プロトコルが想定される。

【0079】

各距離測定について、開始 S T A は、協働 S T A に、不正な応答 S T A が送信した F T M (t_1 $_X$, t_4 $_X$) 物理フレームの到達時刻 t_2 $_X$ として測定されたものについて尋ねる。 $_c$ が添えられている距離は、デバイスによって計算されるものとしての対応する距離である。

開始 S T A はその後、通常通り距離 d を計算する。

$$R T T = [(t_4 _X - t_1 _X) - (t_3 _X - t_2 _X)] \quad (6)$$

2 つのデバイス間の距離は以下のとおりである。

$$d_1 _c = c * R T T / 2 = c * [(t_4 _X - t_1 _X) - (t_3 _X - t_2 _X)] / 2 \quad (7)$$

ここで、 c は光速 (約 $3 * 10^8$ m/s) である。すべての正確が正確に行われ、報

10

20

30

40

50

告されている場合、計算された $d1_c$ は、測定正確度内で現実の距離 d に対応する。

【0080】

不正な応答 STA が、開始 STA に、不正な応答 STA が d ではなく偽装距離 f にあると考えるよう所望すると仮定する。不正な応答 STA は、 $t4_X$ 及び $t1_X$ を測定している。この目的のために、応答 STA は、自身が報告する $t4_r_X$ 及び $t1_r_X$ の値を、それらの距離が、現実には測定される $t4_X$ 及び $t1_X$ の距離未満の $2 * (d - f) / c$ であるように変更する。したがって、不正な応答 STA が開始 STA に報告する時刻は、以下のとおりである。

$$(t4_r_X, t1_r_X) = (t4_X - (1 - \alpha) * (2 * (d - f) / c), t1_X + \alpha * (2 * (d - f) / c)) \quad (8)$$

ここで、 α は自由に選択することができる。

【0081】

応答 STA によって報告されるものとしての $(t4_r_X, t1_r_X)$ を使用することによって、開始 STA は、応答 STA と自身との間の距離 $d1_c$ を、以下のよう

$$\begin{aligned} d1_c &= c * RTT / 2 \\ &= c * [(t4_X - (1 - \alpha) * (2 * (d - f) / c) - (t1_X + \alpha * (2 * (d - f) / c))) - (t3_X - t2_X)] / 2 \\ &= c * [(t4_X - t1_X) - (t3_X - t2_X) - (2 * (d - f) / c)] / 2 \\ &= c * [(t4_X - t1_X) - (t3_X - t2_X)] / 2 - c * (2 * (d - f) / c) / 2 \\ &= d - (d - f) \\ &= f \end{aligned} \quad (9)$$

この計算された距離は、実際、不正な応答 STA が開始 STA に計算することを所望したものである。

【0082】

応答 STA によって報告されるものとしての $(t4_r_X, t1_r_X)$ 及び協働 STA から得られる $t2c_X$ を使用することによって、開始 STA は、応答 STA と協働 STA との間の距離 $d2_c$ を、以下のよう

$$d2_c = d1_c + c * (t2c_X - t2_X) \quad (10)$$

辺 A 、 B 及び C を有する任意の三角形について、以下の不等式が必ず成り立つ（三角不等式）。

$$|C| \leq |A| + |B| \quad (11)$$

したがって、図2の配置において、以下の2つの不等式が、現実の距離及び開始 STA によって測定されるものとしての距離について必ず真である。

$$L \leq d1 + d2 \Leftrightarrow \quad (12)$$

$$L \leq 2 * d1 + c * (t2c_X - t2_X) \quad (13)$$

開始 STA は、上記2つの不等式が、測定距離 $d1_c$ 及び $d2_c$ について成り立つか否かをチェックすることができる。

$$L \leq d1_c + d2_c \Leftrightarrow \quad (14)$$

$$L \leq d1_c + d1_c + c * (t2c_X - t2_X) \Leftrightarrow \quad (15)$$

$$L \leq 2 * f + c * (t2c_X - t2_X) \quad (16)$$

図2の配置において、 $d1$ 及び $d2$ は等しく、そのため、 $t2c_X$ 及び $t2_X$ は等しい。これは、不正な応答 STA が以下のように f を選択する場合、不等式 (16) がもはや成り立たないことを意味する。

$$f < L / 2 \quad (17)$$

これは、図2の配置において、応答 STA が、開始 STA に対して $L / 2$ よりも近くに見えることを所望するようにその測定値を偽装したことを、開始 STA が検出することができることを意味する。

【0083】

図3は、無線通信のための2つのデバイスの空間的配置を示す。配置300は、開始STAと呼ばれる第1のデバイス310と、応答STAと呼ばれる第2のデバイス320と、協働STAと呼ばれる第3のデバイス330とを含み、これらのデバイスは図1を参照しながら説明したデバイスと同様である。第1の距離 $d1_c$ が、現実の距離 $d1$ （又は d ）にある第1のデバイス310と第2のデバイス320との間で決定される。第3の距離 $d2_c$ が、現実の距離 $d2$ にある第3のデバイス330と第2のデバイス320との間で決定される。信用される距離 L が、第1のデバイス310と第3のデバイス330との間にある。

【0084】

この例において、開始STAは不正な応答STAまでの距離として f を測定し、協働STAと不正な応答STAとのあいだの距離として、 $f - L$ を決定する。

ここで、不等式(14)は以下ようになる。

$$L \leq d1_c + d2_c \Leftrightarrow \quad (18)$$

$$L \leq 2 * f - L \Leftrightarrow \quad (19)$$

$$L \leq f \quad (20)$$

これは、 f が L 以上である場合にのみ成り立つ。それゆえ、提案されている防衛は、図3の配置に対して機能し、応答STAが、開始STAに対して L よりも近くに見えることを所望するようにその測定値を偽装したことを、開始STAが検出することができる。

【0085】

図4は、無線通信のための2つのデバイスのさらなる空間的配置を示す。配置400は、開始STAと呼ばれる第1のデバイス410と、応答STAと呼ばれる第2のデバイス420と、協働STAと呼ばれる第3のデバイス430とを含み、これらのデバイスは図1を参照しながら説明したデバイスと同様である。第1の距離 $d1_c$ が、現実の距離 $d1$ （又は d ）にある第1のデバイス410と第2のデバイス420との間で決定される。第3の距離 $d2_c$ が、現実の距離 $d2$ にある第3のデバイス430と第2のデバイス420との間で決定される。信用される距離 L が、第1のデバイス410と第3のデバイス430との間にある。

【0086】

この例においては、余弦法則が使用される。 $d2$ が、以下のように計算される。

$$d2^2 = d1^2 + L^2 - 2 * d1 * L * \cos(\phi) \quad (21)$$

以下のように α を使用して $d1$ 及び L を関係付けることによって、

$$d1 = \alpha * L \quad (22)$$

以下が得られる。

$$d2 = \sqrt{(\alpha * L)^2 + L^2 - 2 * \alpha * L * L * \cos(\phi)}$$

$$= L * \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} \quad (23)$$

しかしながら、不正な応答STAは、開始STAが計算した距離 $d1_c$ 及び $d2_c$ が以下になるように、自身が開始STAに送信する情報を変更する。

$$d1_c = d1 - (d1 - f) \quad (24)$$

$$d2_c = d2 - (d1 - f) \quad (25)$$

開始STAは、自身が測定した距離について、不等式(14)が成り立つか否かをチェックする。

$$L \leq d1_c + d2_c \Leftrightarrow \quad (26)$$

$$L \leq f + L * \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} - \alpha * L + f \Leftrightarrow \quad (27)$$

$$L \leq 2 * f + L * \{\sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} - \alpha\} \Leftrightarrow \quad (28)$$

$$f \geq 0.5 * L * \{1 + \alpha - \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)}\} \quad (29)$$

したがって、開始STAは、応答STAが f を以下の不等式にあるように選択するとき、応答STAがその報告測定値を偽装していることを検出する。

$$f / L < 0.5 * \{1 + \alpha - \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)}\} = T1$$

10

20

30

40

50

(3 0)

表 1 は、 $\alpha \geq 0$ 及び $0 \leq \phi \leq 90$ 度の組み合わせについての T 1 の値を示す。

【 0 0 8 7 】

【表 1】

$\alpha \backslash \phi$	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.10	0.10	0.10	0.09	0.09	0.08	0.07	0.06	0.06	0.05
0.20	0.20	0.20	0.19	0.18	0.17	0.16	0.14	0.12	0.11	0.09
0.30	0.30	0.30	0.29	0.27	0.25	0.23	0.21	0.18	0.15	0.13
0.40	0.40	0.39	0.38	0.36	0.33	0.30	0.26	0.23	0.19	0.16
0.50	0.50	0.49	0.47	0.44	0.40	0.36	0.32	0.27	0.23	0.19
0.51	0.51	0.50	0.48	0.45	0.41	0.37	0.32	0.28	0.23	0.19
0.55	0.55	0.54	0.52	0.48	0.44	0.39	0.34	0.29	0.25	0.20
0.60	0.60	0.59	0.56	0.52	0.47	0.42	0.36	0.31	0.26	0.22
0.70	0.70	0.68	0.64	0.59	0.53	0.47	0.41	0.35	0.29	0.24
0.80	0.80	0.77	0.72	0.65	0.58	0.51	0.44	0.38	0.32	0.26
0.90	0.90	0.85	0.78	0.70	0.62	0.55	0.47	0.40	0.34	0.28
1.00	1.00	0.91	0.83	0.74	0.66	0.58	0.50	0.43	0.36	0.29
1.10	1.00	0.95	0.86	0.77	0.69	0.60	0.52	0.45	0.37	0.31
1.20	1.00	0.96	0.89	0.80	0.71	0.63	0.54	0.46	0.39	0.32
1.30	1.00	0.97	0.90	0.82	0.73	0.65	0.56	0.48	0.40	0.33
1.40	1.00	0.97	0.91	0.83	0.75	0.66	0.58	0.49	0.41	0.34
1.50	1.00	0.98	0.92	0.85	0.76	0.68	0.59	0.50	0.42	0.35
1.60	1.00	0.98	0.93	0.86	0.77	0.69	0.60	0.51	0.43	0.36
1.70	1.00	0.98	0.93	0.86	0.78	0.70	0.61	0.52	0.44	0.36
1.80	1.00	0.98	0.94	0.87	0.79	0.71	0.62	0.53	0.45	0.37
1.90	1.00	0.98	0.94	0.88	0.80	0.71	0.63	0.54	0.46	0.38
2.00	1.00	0.99	0.94	0.88	0.80	0.72	0.63	0.55	0.46	0.38
3.00	1.00	0.99	0.96	0.90	0.84	0.76	0.68	0.59	0.50	0.42
4.00	1.00	0.99	0.96	0.91	0.85	0.78	0.70	0.61	0.52	0.44
5.00	1.00	0.99	0.96	0.92	0.86	0.79	0.71	0.62	0.54	0.45

10

20

30

40

50

6.00	1.00	0.99	0.96	0.92	0.86	0.79	0.72	0.63	0.55	0.46
7.00	1.00	0.99	0.97	0.92	0.87	0.80	0.72	0.64	0.55	0.46
8.00	1.00	0.99	0.97	0.92	0.87	0.80	0.73	0.64	0.56	0.47
9.00	1.00	0.99	0.97	0.93	0.87	0.80	0.73	0.65	0.56	0.47
10.00	1.00	0.99	0.97	0.93	0.87	0.81	0.73	0.65	0.56	0.48
100.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.58	0.50
1000.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.59	0.50

10

表 2 は、 $\alpha \geq 0$ 及び $90 \leq \phi \leq 180$ 度の組み合わせについての T 1 の値を示す。
【 0 0 8 8 】
【表 2】

ϕ α	90.0	100.0	110.0	120.0	130.0	140.0	150.0	160.0	170.0	180.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.05	0.04	0.03	0.02	0.02	0.01	0.01	0.00	0.00	0.00
0.20	0.09	0.07	0.06	0.04	0.03	0.02	0.01	0.01	0.00	0.00
0.30	0.13	0.10	0.08	0.06	0.04	0.03	0.02	0.01	0.00	0.00
0.40	0.16	0.13	0.10	0.08	0.05	0.03	0.02	0.01	0.00	0.00
0.50	0.19	0.15	0.12	0.09	0.06	0.04	0.02	0.01	0.00	0.00

20

30

40

50

0.60	0.22	0.17	0.13	0.10	0.07	0.05	0.03	0.01	0.00	0.00
0.70	0.24	0.19	0.15	0.11	0.08	0.05	0.03	0.01	0.00	0.00
0.80	0.26	0.21	0.16	0.12	0.08	0.05	0.03	0.01	0.00	0.00
0.90	0.28	0.22	0.17	0.13	0.09	0.06	0.03	0.01	0.00	0.00
1.00	0.29	0.23	0.18	0.13	0.09	0.06	0.03	0.02	0.00	0.00
1.10	0.31	0.25	0.19	0.14	0.10	0.06	0.04	0.02	0.00	0.00
1.20	0.32	0.25	0.20	0.15	0.10	0.07	0.04	0.02	0.00	0.00
1.30	0.33	0.26	0.20	0.15	0.11	0.07	0.04	0.02	0.00	0.00
1.40	0.34	0.27	0.21	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.50	0.35	0.28	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.60	0.36	0.29	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.70	0.36	0.29	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.80	0.37	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.90	0.38	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
2.00	0.38	0.31	0.24	0.18	0.12	0.08	0.05	0.02	0.01	0.00
3.00	0.42	0.34	0.26	0.20	0.14	0.09	0.05	0.02	0.01	0.00
4.00	0.44	0.36	0.28	0.21	0.15	0.10	0.05	0.02	0.01	0.00
5.00	0.45	0.37	0.29	0.22	0.15	0.10	0.06	0.03	0.01	0.00
6.00	0.46	0.37	0.29	0.22	0.16	0.10	0.06	0.03	0.01	0.00
7.00	0.46	0.38	0.30	0.23	0.16	0.10	0.06	0.03	0.01	0.00
8.00	0.47	0.38	0.30	0.23	0.16	0.11	0.06	0.03	0.01	0.00
9.00	0.47	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
10.00	0.48	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
100.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00
1000.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00

応答 S T A が、距離 $0.5 * L$ 以下にあると偽装することを所望していることを検出することが関心事であると仮定する。そのため、偽装 S T A ($0.5 L$ よりも遠い) が $0.5 L$ よりも近くに見えることを所望する場合、これは、偽装 S T A が網掛けのない領域内にある場合に検出することができる。そのため、これらの偽装 S T A の測定距離は、それらの意図するところであるため、 $0.5 L$ 未満である。

【0089】

S T A が実際に $0.5 * L$ 以内にある場合、偽装する必要はなく、そのため、表 1 において $\alpha \leq 0.5$ の領域は網掛けされていない。

【0090】

表 1 及び表 2 の灰色の網掛け領域は、応答 S T A と開始 S T A との間の現実の距離が $0.5 * L$ よりも大きく（したがって、 $\alpha > 0.5$ ）、応答 S T A が $0.5 * L$ 以下の距離にあるように見えることを所望していることを開始 S T A が検出することができないところである。提案されている方法は、 $0 \leq \phi \leq 90$ 度の大きい領域内に存在する不正な応答 S T A に対して保護する。しかしながら、方法は、 $90 < \phi \leq 180$ 度の領域内の不正な応答 S T A については保護しない。そのために、さらなる協働デバイスを使用することが提案される。そのため、距離を測定するためのシステムは、第 1 のデバイスと、少なくとも 2 つの協働デバイスとを含む。様々な例が下記に論じられる。そのようなシステムにおいて、第 2 の協働デバイスと動作する第 4 のデバイスは、第 4 のメッセージプロセッサであって、第 4 のデバイスにおける測定メッセージの第 4 の到達時刻を決定することと、第 4 のサポートデータを第 1 のデバイスに転送することであって、第 4 のサポートデータは、第 4 の到達時刻に基づく、転送することを行うように構成されている、第 4 のメッセージプロセッサを有する。第 1 のメッセージプロセッサは、第 2 の協働デバイスから第 4 のサポートデータを受信することと、第 4 のサポートデータを使用して第 4 のデバイスと第 2 のデバイスとの間の第 4 の距離を得ることと、第 2 の信用される距離及び第 4 の距離も使用して検証テストを実施することとを行うように構成されている。

【0091】

一実施形態において、検証テストは、第 1 のデバイス、第 2 のデバイス及び第 3 のデバイスの第 1 の空間的配置に関する第 1 の三角不等式と、第 1 のデバイス、第 2 のデバイス及び第 4 のデバイスの第 2 の空間的配置に関する第 2 の三角不等式との組み合わせを使用する。検証テストは、下記の三角不等式及び 2 つの協働 S T A を使用することに関するセクションにおいて論じられているテストを含む。代替的に、検証テストは、三角不等式及び 2 つの協働 S T A をより良好に使用することに関する後のセクションにおいて説明されているような 2 つの協働 S T A を使用する。このために、2 つの協働デバイス間の距離が、第 1 のデバイスに知られる。

【0092】

一実施形態において、検証テストは、第 1 の空間的配置による第 2 のデバイスの第 1 の位置が第 2 の空間的配置による第 2 のデバイスの第 2 の位置に対応するか否かを検証する。任意選択的に、検証テストは、決定された距離のすべてがゼロよりも大きいか否かを決定するための非一貫性チェックを使用する。

【0093】

また、検証テストは、第 1 の信頼できる距離及び第 2 の信用される距離を超えるものに基づき、すなわち、第 1 のデバイス、第 3 のデバイス及び第 4 のデバイスから成る配置全体に基づく。例えば、これは、開始デバイスと両方の協働デバイスとの間の接続線の間の信用される角度を使用して行うことができる。任意選択的に、検証テストは、第 3 のデバイスから第 1 のデバイスへの線と、第 4 のデバイスから第 1 のデバイスへの線との間の信頼できる角度が少なくとも 90 度になるように、第 3 のデバイス及び第 4 のデバイスが配置される構成に基づく。任意選択的に、検証テストは、第 3 のデバイス及び第 4 のデバイスが第 1 のデバイスに関して互いに対向して配置される構成に基づく。任意選択的に、検証テストは、第 2 の信用される距離が信用される距離に対応する構成に基づく。検証テストの様々な状況及び計算は、以下のセクションにおいて論じる。以下の例は、三角不等式及び 2 つの協働 S T A を使用する。

【0094】

図 5 は、2 つの協働デバイスを有する空間的配置を示す。配置 500 は、「開始 S T A」とマークされている第 1 のデバイスと、図 1 を参照しながら説明したデバイスと同様の 2 つの「協働 S T A」とを含む。第 1 の信用される距離 L が第 1 のデバイスと第 1 の協働 S T A との間にあり、一方、第 2 の信用される距離 L が第 1 のデバイスと第 2 の協働 S T A との間にある。

【0095】

この例示的な配置を使用すると、第 1 の協働 S T A に正確に対向する第 2 の協働 S T A

を使用することによって、 $90 < \phi \leq 180$ についてより良好な性能が達成される。その場合、開始 S T A は、すべてではないが多数の、 $0.5 * L$ よりも近くに見えることを所望する、不正な応答 S T A を検出することができる。この配置について、 $0.5 L$ 以下の距離にあるように偽装することを所望している応答 S T A がある領域は、図 5 において灰色で示されている。この領域は、断面がくさび形のリングのように見える。

【0096】

図 6 は、2つの協働デバイスを有する第 2 の空間的配置を示す。配置 600 は、開始 S T A と呼ばれる第 1 のデバイスと、図 1 を参照しながら説明したデバイスと同様の 2つの協働 S T A とを含む。第 1 の信用される距離 L が第 1 のデバイスと第 1 の協働 S T A との間にあり、一方、第 2 の信用される距離 L が第 1 のデバイスと第 2 の協働 S T A との間に

10

【0097】

この例示的な配置を使用して、開始 S T A は、2つの協働 S T A を上述したように使用し、応答 S T A が、距離 $0.3 * L$ 以下にあると偽装することを所望していることに関心がある。その場合、表 1 から、少なくとも $1.1 L$ 離れているすべての応答 S T A、及び、 $1.1 L$ よりも近い多くの S T A が捕捉されることが分かる。

【0098】

図 7 は、2つの協働デバイスを有するさらなる空間的配置を示す。配置 700 は、開始 S T A と呼ばれる第 1 のデバイス 710 と、応答 S T A と呼ばれる第 2 のデバイス 720 と、図 1 を参照しながら説明したデバイスと同様の 2つの協働 S T A 730、731 とを含む。第 1 の信用される距離 L が第 1 のデバイスと第 1 の協働 S T A との間にあり、一方、第 2 の信用される距離 L が第 1 のデバイスと第 2 の協働 S T A との間にある。この特定の配置において、第 2 のデバイス 720 は、 $3d$ において、その中心が第 1 のデバイス、第 3 のデバイス及び第 4 のデバイスを通る線上にある円上のどこにあることもできることに留意されたい。このため、ここでは、第 2 のデバイスの位置は、第 1 のデバイス、第 3 のデバイス及び第 4 のデバイスを通る平面内の $2d$ 座標としてのみ計算する。

20

【0099】

この例示的な配置においては、三角不等式及び 2つの協働 S T A が使用される。三角不等式は、協働 S T A 1 及び 2 を介した測定に対して使用される。余弦法則を使用すると、 d_{2_1} を以下のように計算することができる。

30

$$d_{2_1}^2 = L * \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} \quad (31)$$

また、 d_{2_2} は以下のとおりである。

$$\begin{aligned} d_{2_2}^2 &= L * \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(180 - \phi)} \\ &= L * \sqrt{\alpha^2 + 1 + 2 * \alpha * \cos(\phi)} \end{aligned} \quad (32)$$

不正な応答 S T A は、開始 S T A が計算した距離 d_{1_c} 、 $d_{2_1_c}$ 及び $d_{2_2_c}$ が以下になるように、自身が開始 S T A に送信する情報を変更する。

$$d_{1_c} = d_1 - (d_1 - f) \quad (33)$$

$$d_{2_1_c} = d_{2_1} - (d_1 - f) \quad (34)$$

$$d_{2_2_c} = d_{2_2} - (d_1 - f) \quad (35)$$

開始 S T A は、自身が協働 S T A 1 及び 2 から受信した距離について、不等式 (14) が成り立つか否かをチェックする。

40

$$2 * L \leq d_{2_1_c} + d_{2_2_c} \Leftrightarrow \quad (36)$$

$$2 * L \leq L * \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} + L * \sqrt{\alpha^2 + 1 + 2 * \alpha * \cos(\phi)} - 2 * (\alpha * L - f) \Leftrightarrow \quad (37)$$

$$L \leq f + L * \{ \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} + \sqrt{\alpha^2 + 1 + 2 * \alpha * \cos(\phi)} - 2 * \alpha \} / 2 \Leftrightarrow \quad (38)$$

$$s f \geq 0.5 * L * \{ 2 + 2 * \alpha - \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} - \sqrt{\alpha^2 + 1 + 2 * \alpha * \cos(\phi)} \} \Leftrightarrow \quad (39)$$

したがって、開始 S T A は、応答 S T A が f を以下の不等式にあるように選択するとき、応答 S T A がその報告測定値を偽装していることを検出する。

50

$$f/L < 0.5 * \{ 2 + 2 * \alpha - \sqrt{\alpha^2 + 1 - 2 * \alpha * \cos(\phi)} \} - \sqrt{\alpha^2 + 1 + 2 * \alpha * \cos(\phi)} = T3 \quad (40)$$

表3は、 $\alpha \geq 0$ 及び $0 \leq \phi \leq 180$ 度の組み合わせについてのT1の値を示す。T3の値の表は、 $\phi = 90$ 度を中心として対称である。

【0100】

【表3】

φ α	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0.20	0.20	0.20	0.20	0.19	0.19	0.19	0.18	0.18	0.18	0.18
0.30	0.30	0.30	0.29	0.29	0.28	0.27	0.27	0.26	0.26	0.26
0.40	0.40	0.40	0.39	0.38	0.36	0.35	0.34	0.33	0.32	0.32
0.50	0.50	0.50	0.48	0.46	0.44	0.42	0.41	0.39	0.38	0.38
0.51	0.51	0.50	0.49	0.47	0.45	0.43	0.41	0.40	0.39	0.39
0.55	0.55	0.54	0.53	0.50	0.48	0.46	0.44	0.42	0.41	0.41
0.60	0.60	0.59	0.57	0.54	0.51	0.49	0.46	0.45	0.44	0.43
0.70	0.70	0.69	0.65	0.61	0.58	0.54	0.52	0.50	0.48	0.48
0.80	0.80	0.78	0.73	0.68	0.63	0.59	0.56	0.54	0.52	0.52
0.90	0.90	0.86	0.79	0.73	0.68	0.63	0.60	0.57	0.56	0.55
1.00	1.00	0.92	0.84	0.78	0.72	0.67	0.63	0.61	0.59	0.59
1.10	1.00	0.95	0.88	0.81	0.75	0.70	0.66	0.64	0.62	0.61
1.20	1.00	0.97	0.90	0.84	0.78	0.73	0.69	0.66	0.64	0.64
1.30	1.00	0.97	0.92	0.86	0.80	0.75	0.71	0.68	0.67	0.66
1.40	1.00	0.98	0.93	0.87	0.82	0.77	0.73	0.70	0.69	0.68
1.50	1.00	0.98	0.94	0.89	0.83	0.79	0.75	0.72	0.70	0.70
1.60	1.00	0.99	0.95	0.90	0.85	0.80	0.76	0.74	0.72	0.71
1.70	1.00	0.99	0.95	0.91	0.86	0.81	0.78	0.75	0.73	0.73
1.80	1.00	0.99	0.96	0.91	0.87	0.83	0.79	0.76	0.75	0.74

10

20

30

40

50

1.90	1.00	0.99	0.96	0.92	0.88	0.84	0.80	0.77	0.76	0.75
2.00	1.00	0.99	0.96	0.93	0.88	0.84	0.81	0.79	0.77	0.76
3.00	1.00	0.99	0.98	0.96	0.93	0.90	0.87	0.85	0.84	0.84
4.00	1.00	1.00	0.98	0.97	0.95	0.93	0.91	0.89	0.88	0.88
5.00	1.00	1.00	0.99	0.97	0.96	0.94	0.92	0.91	0.90	0.90
6.00	1.00	1.00	0.99	0.98	0.97	0.95	0.94	0.93	0.92	0.92
7.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.93	0.93
8.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.94	0.94
9.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.95	0.95	0.94
10.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.96	0.95	0.95
100.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
1000.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

10

20

応答 S T A が、距離 $0.5 * L$ 以下にあると偽装することを所望していることを検出することが関心事であると仮定する。S T A が実際に $0.5 * L$ 以内にある場合、偽装する必要はなく、そのため、表 3 において $\alpha \leq 0.5$ の領域は網掛けされていない。

【0101】

表 3 の灰色の網掛け領域は、応答 S T A と開始 S T A との間の現実の距離が $0.5 * L$ よりも大きく（したがって、 $\alpha > 0.5$ ）、応答 S T A が $0.5 * L$ 以下の距離にあるように見えることを所望していることを開始 S T A が検出することができないところである。提案されている方法が、 $0 \leq \phi \leq 90$ 度の大きい領域内に存在する不正な応答 S T A に対して保護すること、及び、方法が保護しない領域（灰色の網掛け領域）は、表 1 のものよりも明らかに小さく小さいことは明らかである。

30

【0102】

図 7 の配置において、複数の様態で 4 つのデバイスを通る平面内の位置 (x, y) を計算することが可能である。応答 S T A がその測定値を忠実に報告する場合、これらの計算されている位置は、測定誤差を除いて一致する。しかし、応答 S T A がその測定値を偽装している場合、特に、応答 S T A が現実にもうであるよりも近くに見えることを所望するとき、それらの位置は一致しない。

40

【0103】

開始 S T A が $(x, y) = (0, 0)$ にあり、協働 S T A 1 が $(L, 0)$ にあり、協働 S T A 2 が $(-L, 0)$ にあると仮定する。これらの S T A 及び応答 S T A は無論、3 - d 世界に位置することに留意されたい。平面 (x, y) は、開始 S T A 及び 2 つの協働 S T A を通る線が存在する 3 - d 内の任意の平面であってもよい。このセクションにおける y 座標の計算が、2 つの値 $\pm y$ をもたらしたはずである。正の解のみを保持することは何ら問題を呈しない。これは、平面が開始 S T A 及び 2 つの協働 S T A を通る線を中心に 180 度回転されたときに、 y の他方の解が得られるためである。

【0104】

最初に、下記のセクション「余弦法則チェックと三角不等式チェックとの間の関連」に

50

において説明されているように、開始 S T A によって決定された距離が、ゼロよりも大きい
か否かがチェックされる。

$$d1_c > 0 \quad (41)$$

$$d2_1_c > 0 \quad (42)$$

$$d2_2_c > 0 \quad (43)$$

上記3つの不等式のいずれも当てはまらない場合、応答 S T A が不正であると仮定する。
これら3つの不等式が当てはまる場合、以下のように、辺の4つの組み合わせについて
、余弦法則を使用して、応答 S T A の位置を計算する。

$$\cos(\angle ACB) = (|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|) \quad (44)$$

点 b を常に応答 S T A の位置として使用する。

【0105】

点 a = (L, 0) 及び c = (0, 0) を使用すると、応答 S T A が b1 = (x1, y1)
にあると測定することができる。

$$\cos_c1 = (d1_c^2 + L^2 - d2_1_c^2) / (2 * d1_c * L) \quad (45)$$

点 a = (-L, 0) 及び c = (0, 0) を使用すると、応答 S T A が b = (x2, y2)
にあると測定することができる。

$$\cos_c2 = (d1_c^2 + L^2 - d2_2_c^2) / (2 * d1_c * L) \quad (46)$$

点 a = (L, 0) 及び c = (-L, 0) を使用すると、応答 S T A が b = (x3, y3)
にあると測定することができる。

$$\cos_c3 = (d2_1_c^2 + 4L^2 - d2_2_c^2) / (2 * d2_1_c * 2L) \quad (47)$$

点 a = (-L, 0) 及び c = (L, 0) を使用すると、応答 S T A が b = (x4, y4)
にあると測定することができる。

$$\cos_c4 = (d2_2_c^2 + 4L^2 - d2_1_c^2) / (2 * d2_2_c * 2L) \quad (48)$$

その後、計算された余弦の4つすべてが間隔 [-1, 1] 内にあるか否かをチェックす
る。下記のセクション「余弦法則チェックと三角不等式チェックとの間の関連」から、こ
こまでで三角不等式テストと同じテストを実施しており、そのため、ここまでのチェック
によって、上記3つのテーブルが適用される。

4つの計算されている余弦がすべて間隔 [-1, 1] 内にある場合、以下のように、応
答 S T A の位置の4つの点 b1、b2、b3 及び b4 を以下のように計算する。

$$x1 = \cos_c1 * d1_c \quad (49)$$

$$y1 = \sqrt{1 - \cos_c1^2} * d1_c \quad (50)$$

$$x2 = -\cos_c2 * d1_c \quad (51)$$

$$y2 = \sqrt{1 - \cos_c2^2} * d1_c \quad (52)$$

$$x3 = L - \cos_c3 * d2_1_c \quad (53)$$

$$y3 = \sqrt{1 - \cos_c3^2} * d2_1_c \quad (54)$$

$$x4 = -L + \cos_c4 * d2_2_c \quad (55)$$

$$y4 = \sqrt{1 - \cos_c4^2} * d2_2_c \quad (56)$$

応答 S T A がその時間測定値を忠実に報告した場合、これら4つの点は、タイミング測
定誤差の影響を除いて同じであるはずである。同じく他の箇所で説明されるように、測定
を複数回実施し、結果を平均することによって、測定誤差をより小さくすることができ
ることに留意されたい。しかしながら、これら4つの点は、応答 S T A がその測定値を現実
にそうであるよりも近くに見えるように偽装するとき、及び、応答 S T A が協働 S T A 1
及び 2 を通る線上にないとき、互いに異なる。

4つの点 b1、b2、b3 及び b4 の間のすべての距離の最大値 e m a x を計算する。

$$i \in \{1, 2, 3, 4\} \text{ 及び } j \in \{1, 2, 3, 4\} \text{ について } e m a x = \text{MAX} | b i$$

10

20

30

40

50

− b j | (5 7)

b 3 及び b 4 は数値誤差を除いて同じ点として計算されるため、 b 4 を計算する必要はないことに留意されたい。

【 0 1 0 6 】

表 4 は、余弦チェックのいずれもが失敗する場合を除く e m a x / L の値を示しており、その場合、 9 9 の値が示されている。不正な応答 S T A が見えることを所望する値 f が、これらのチェックにとって重要である。表 4 においては f を 0 . 9 になるように選択している。

【 0 1 0 7 】

【表 4】

$\phi \backslash \alpha$	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
180.0	180.0	170.0	160.0	150.0	140.0	130.0	120.0	110.0	100.0	90.0
0.00	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85
0.10	1.65	1.59	1.55	1.53	1.50	1.48	1.47	1.46	1.45	1.45
0.20	1.46	1.38	1.31	1.27	1.23	1.20	1.18	1.16	1.15	1.15
0.30	1.26	1.16	1.09	1.03	0.99	0.95	0.93	0.91	0.90	0.89
0.40	1.07	0.96	0.87	0.81	0.77	0.73	0.71	0.69	0.68	0.68
0.50	0.87	0.76	0.67	0.61	0.57	0.54	0.52	0.50	0.50	0.49
0.51	0.85	0.74	0.65	0.59	0.55	0.52	0.50	0.49	0.48	0.48
0.55	0.77	0.66	0.57	0.51	0.48	0.45	0.43	0.42	0.42	0.41
0.60	0.68	0.56	0.48	0.42	0.39	0.37	0.36	0.35	0.34	0.34
0.70	0.48	0.36	0.30	0.26	0.24	0.23	0.22	0.21	0.21	0.21
0.80	0.28	0.18	0.14	0.12	0.11	0.10	0.10	0.10	0.10	0.10
0.90	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
1.00	99.00	99.00	0.11	0.10	0.09	0.09	0.09	0.08	0.08	0.08
1.10	99.00	99.00	0.21	0.18	0.17	0.16	0.16	0.16	0.16	0.15
1.20	99.00	99.00	99.00	0.25	0.23	0.22	0.22	0.22	0.22	0.22
1.30	99.00	99.00	99.00	0.31	0.29	0.28	0.28	0.27	0.27	0.27
1.40	99.00	99.00	99.00	0.36	0.34	0.33	0.32	0.32	0.32	0.32
1.50	99.00	99.00	99.00	0.41	0.38	0.37	0.36	0.36	0.36	0.36
1.60	99.00	99.00	99.00	0.47	0.42	0.41	0.40	0.40	0.40	0.40
1.70	99.00	99.00	99.00	99.00	0.46	0.44	0.43	0.43	0.44	0.44
1.80	99.00	99.00	99.00	99.00	0.49	0.47	0.46	0.46	0.47	0.47

10

20

30

40

50

1.90	99.00	99.00	99.00	99.00	0.52	0.50	0.49	0.49	0.49	0.49
2.00	99.00	99.00	99.00	99.00	0.56	0.53	0.51	0.52	0.52	0.52
3.00	99.00	99.00	99.00	99.00	99.00	0.80	0.72	0.68	0.68	0.68
4.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	0.84	0.78	0.76
5.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
6.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
7.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
8.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
9.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
10.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
100.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
1000.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00

10

20

【0108】

この表から分かるように、 $\alpha > 0.9$ について、99を示すセルは表3の0.9を超える値を有するセルと一致しており、これは、下記のセクション「余弦法則チェックと三角不等式チェックとの間の関連」に論じられている等価性を示す。実際に開始STAから0.9Lの距離内にある応答STAは、この範囲内にあると偽装する必要がなく、そのため、この領域は表4において網掛けされていない。0.25Lを、応答STAの位置の測定値b1、b2、b3及びb4の最大不一致の閾値として使用して、セルが0.25未満の値を有し、 $\alpha > 0.9$ である表4の領域を網掛けした。

30

【0109】

これは、網掛け領域において、そのため、開始STAから0.9L～1.2Lの距離を有する応答STAについて基本的に、提案されているシステムは、これらの応答STAが、それらのタイミング測定値を開始STAから0.9L以内に位置するように見えるように偽装していると判定することができないことを意味する。

【0110】

したがって、開始STAから距離Lにある対向する位置に配置されている2つの協働STAを使用して、提案されているシステムは、開始STAから1.2Lよりも大きいすべての距離に位置する応答STAが、開始STAから0.9L以内に位置するように見えるように偽装していると判定することができる。

40

【0111】

以下のセクションは、三角不等式及び3つ以上の協働STAを使用する。3つ以上の協働STAを開始STAの周りに配置することによって、より良好な性能が得られる。開始STAの可能な限り多くの位置に配置されている不正な応答STAを最良に検出するためには、3つの協働STAを使用するとき、開始STA及び協働STAを1つの平面内に配置することが最良である。それは、開始STAが3つの協働STAを通る平面上にない場合、不正な応答STAが常に3つの協働STAのいずれよりも開始STAの近くにあり、したがって、提案されている方法が機能しないボリュームが存在するためである（例え

50

ば、表 2 参照)。

【0112】

1つの線上に位置決めされていないが、その配置が三角形を形成する、2つの協働 S T A 及び1つの開始 S T Aを使用することも可能である。距離 d 1、d 2 __ 1、d 2 __ 2 並びに2つの協働 S T A 及び開始 S T A によって形成される三角形の辺の長さを使用して、開始 S T A は、第2のデバイスと、2つの協働 S T A 及び開始 S T A から成るセットからのデバイスの任意の対とによって形成される三角形に関する余弦法則を使用したチェックを実施することができる。

【0113】

4つの協働 S T Aを使用するとき、それらは理想的には、正四面体の角に配置されるべきであり、開始 S T A は、正四面体の重心に配置される。この配置は、可能性のある最も対称なものであり、したがって、最良の保護を提供する。

その4点が単位球面上にあり、原点に重心があり、水平な下面レベルを有する正四面体の頂点は、以下ようになる。

$$A = (\sqrt{8/9}, 0, -1/3)$$

$$B = (-\sqrt{2/9}, \sqrt{2/3}, -1/3)$$

$$C = (-\sqrt{2/9}, -\sqrt{2/3}, -1/3)$$

$$D = (0, 0, 1)$$

したがって、この場合、協働 S T A は、頂点の位置に配置され、開始 S T A は、原点に配置され、距離 L は1に等しい。任意の2つの S T A 間の最長距離は、任意の2つの協働 S T A 間の距離であり、そのため、以下のような、正四面体の辺の各々の長さである。

$$\begin{aligned} ||A-D|| &= ||(\sqrt{8/9}, 0, -1/3) - (0, 0, 1)|| \\ &= ||(\sqrt{8/9}, 0, -4/3)|| \\ &= \sqrt{8/3} \quad 1.63 \quad (58) \end{aligned}$$

任意の協働 S T A、原点及び応答 S T A 間の角は、応答 S T A が、原点及び正四面体の4つの面のいずれかの重心を通る線にあるときに最大になる。面 A B D の重心は、以下のとおりである。

$$\begin{aligned} F &= \{(\sqrt{8/9}, 0, -1/3) + (-\sqrt{2/9}, \sqrt{2/3}, -1/3) + (0, 0, 1)\} / 3 \\ &= (\sqrt{8/9} - \sqrt{2/9}, \sqrt{2/3}, 1/3) / 3 \quad (59) \end{aligned}$$

角 $\angle A O F$ 、 $\angle B O F$ 及び $\angle D O F$ はすべて同じである。この角度は、余弦法則を使用して計算することができる。

$$\cos(\angle D O F) = (||D||^2 + ||F||^2 - ||D-F||^2) / (2 * ||D|| * ||F||) \quad (60)$$

$$||D||^2 = 1 \quad (61)$$

$$||F||^2 = \{(\sqrt{8/9} - \sqrt{2/9})^2 + 2/3 + 1/9\} / 9$$

$$= \{8/9 + 2/9 - 2 * \sqrt{16/81} + 7/9\} / 9$$

$$= 1/9 \quad (62)$$

$$||D-F||^2 = \{(\sqrt{8/9} - \sqrt{2/9})^2 + 2/3\} / 9 + (8/9)^2$$

$$= \{8/9 + 2/9 - 2 * \sqrt{16/81} + 2/3\} / 9 + 64/81$$

$$= \{2/9 + 6/9\} / 9 + 64/81$$

$$= 72/81 = 8/9 \quad (63)$$

したがって、

$$\cos(\angle D O F) = (1 + 1/9 - 8/9) / (2 * 1 * 1/3)$$

$$= 3 * (2/9) / 2$$

$$= 1/3 \quad (64)$$

$$\angle D O F = \arccos(1/3) = 70.53 \text{度} \quad (65)$$

10

20

30

40

50

したがって、正四面体の重心に位置する1つの開始STA及び開始STAから距離Lにあるその正四面体の頂点に位置する4つの協働STAから成る配置によって、開始STAまで0.5Lよりも近くにあるように偽装することを所望するすべての応答STAを、それらが開始STAから1.5Lよりも離れている場合に、検出することができる。表1を参照されたい。0.5Lと1.5Lとの間の領域内の多くのそのようなSTAを検出することができる。

【0114】

任意選択的に、この防衛は、前のセクションにおいて説明した防衛と同様の、開始STA及び協働STAを使用した、計算されている位置における非一貫性チェックを追加することによって改善される。

【0115】

一実施形態において、測距プロトコルは、第1のデバイスが、開始デバイスとして動作し、第2のデバイスに開始メッセージを送信することを含み、一方、開始メッセージが受信されると、第2のデバイスは、測定メッセージを送信する必要がある。第1のメッセージプロセッサは、第3のデバイスが距離測定のために開始デバイスとして動作することを可能にするために、第3のデバイスと役割変更データを交換するように構成されている。そのために、第3のデバイスは、役割変更データを受信すると、第2の測定メッセージに基づいて測距プロトコルに従って第3のデバイスと第2のデバイスとの間の距離を取得し、第3のサポートデータを第1のデバイスに転送するように構成されており、第3のサポートデータは、第3の距離を示す。例えば、第3のサポートデータは、第3のデバイスが測定したFTMプロトコルの t_2 及び t_3 値を含む。 t_1 及び t_4 値もその一部であるが、第1のデバイスが第2のデバイスから t_1 及び t_4 を含む元のメッセージを受信及び使用するため、これは必須ではない。

【0116】

また、第1のメッセージプロセッサは、第1のデバイスにおいて第2の測定メッセージを受信するときの第1のデバイスと第2のデバイスとの間の第2の距離を決定し、第3のデバイスから第3のサポートデータを受信し、第2の距離及び第3のサポートデータも使用して検証テストを実施するように構成されている。この実施形態において、開始STA及び協働STAは役割を交換し、又は言い換えれば、2つの開始STAを使用して位置を2度計算する。

【0117】

図4の配置において、ここで、協働して応答STAまでの距離を決定する、第1のSTA1及び第2のSTA2として動作する、2つのデバイス410、430がある。連続する測定において、STA1は開始STAとして動作し、STA2は協働STAとして動作し、第2の連続する測定において、それらは反対の役割を担う。距離測定結果を改善するために、距離を計算する前に、各連続における個々の時間測定値が平均される。第1の連続のすべての個々の測定が行われた後、役割が交換され、第2の連続の個々の測定が実施される。しかし、役割交換はまた、任意の回数の個々の測定の後にも行われる。

【0118】

第1の連続する測定、したがってSTA1が開始STAである測定からのタイミング測定値を使用すると、式(49)及び(50)を使用して応答STAの位置 $r_1 = (x_1, y_1)$ を計算することができる。第2の連続する測定、したがってSTA2が開始STAである測定からのタイミング測定値を使用すると、同様の式を使用して応答STAの位置 $r_2 = (x_2, y_2)$ を計算することができる。この特定の配置において、第2のデバイス420は、3dにおいて、その中心が第1のデバイス及び第3のデバイスを通る線上にある円上のどこにあることもできることに留意されたい。このため、ここでは、第2のデバイスの位置は、第1のデバイス、第2のデバイス及び第3のデバイスを通る平面内の2d座標としてのみ計算する。

【0119】

計算されている点 r_1 及び r_2 は、応答STAがそのタイミング測定値を忠実に報告す

10

20

30

40

50

る場合、測定誤差を除いて等しいはずである。しかし、応答 S T A が現実にも近づくように見えることを所望するとき、これは異なる。

【0120】

前のセクションにおいて、不正な応答 S T A が、開始 S T A から距離 f に見えるように試行している。応答 S T A は、2つの S T A が時折役割を交換していることを知らず、したがって、それらの各々から偽装の距離 f に見えるように試行していると仮定する。この場合、特に $f < 0.5L$ の場合、 r_1 及び r_2 は明らかに異なる。

【0121】

したがって、各々が開始 S T A としての役割を果たす2つ以上の S T A を使用し、開始 S T A の各々によって測定される距離を使用しての位置を計算し、計算されている位置の差を判定することは、それらのタイミング測定値を偽装している応答 S T A を検出するための良好な着想である。

【0122】

しかしながら、上述した攻撃は、この状況における可能な最良の攻撃ではない。応答 S T A が、いずれの開始 S T A と F T M プロトコルを実施しており、配置のパラメータ（したがって L 及び ϕ 又は d_1 及び d_2 ）を知っているときに、攻撃はより良好になる。これが実際に知ることは困難であるが、不可能ではない。攻撃者が、秘密暗号鍵を除いてすべてを知っていると仮定することは、良好なセキュリティ実務である。したがって、前のセクションにおいて説明したような防衛が、好ましくは使用される。

【0123】

以下のセクションは、余弦法則チェックと三角不等式チェックとの間の関連を論じる。以下のような、三角不等式が3つの長さ $|A|$ 、 $|B|$ 及び $|C|$ に当てはまるか否かは、

$$|C| \leq |A| + |B| \quad (66)$$

$$|A| \leq |B| + |C| \quad (67)$$

$$|B| \leq |A| + |C| \quad (68)$$

以下が成り立つか否かのチェックと同じである。

$$-1 \leq \cos(\angle ACB) \leq 1 \quad (69)$$

角 $\angle ACB$ に対する余弦法則は以下のとおりである。

$$\cos(\angle ACB) = (|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|) \quad (70)$$

余弦が -1 以上であるか否かをチェックすることによって、以下が得られる。

$$\begin{aligned} \cos(\angle ACB) \geq -1 &\Leftrightarrow \\ (|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|) &\geq -1 \quad (71) \\ |A| * |B| > 0 \text{ である場合にのみ、不等式 (71) から以下の不等式を導出} & \\ \text{ことができる。} & \end{aligned}$$

$$\begin{aligned} (|A|^2 + |B|^2 - |C|^2) &\geq -2 * |A| * |B| \Leftrightarrow \\ (|A|^2 + |B|^2 + 2 * |A| * |B| - |C|^2) &\geq 0 \Leftrightarrow \\ (|A| + |B|)^2 - |C|^2 &\geq 0 \Leftrightarrow \\ (|A| + |B|)^2 &\geq |C|^2 \Rightarrow \\ |C| &\leq (|A| + |B|) \quad (72) \end{aligned}$$

これは不等式 (66) と同じである。

同様に、余弦が 1 以下であるか否かをチェックすることによって、以下が得られる。

$$\begin{aligned} \cos(\angle ACB) \leq 1 &\Leftrightarrow \\ (|A| - |B|)^2 - |C|^2 &\leq 0 \Leftrightarrow \\ (|A| - |B|)^2 &\leq |C|^2 \Leftrightarrow \\ \text{abs}(|A| - |B|) &\leq |C| \Leftrightarrow \\ |A| &\leq (|B| + |C|) \text{ 且つ } |B| \leq (|A| + |C|) \quad (73) \end{aligned}$$

この2つの不等式は三角形にも当てはまらなければならない。

【0124】

現実の距離は常に 0 以上であることに留意されたい。上記の論法は正の距離には当ては

まるが、負の距離には当てはまらない。応答 S T A がその測定値をより近くなるように偽装するとき、開始 S T A によって得られる距離は負になる場合がある。したがって、3つの三角不等式に関するチェックは、測定されている3つの距離が0以上であるか否かのチェック、及び、余弦不等式(69)が当てはまるか否かのチェックと等価である。

【0125】

一実施形態において、第3のメッセージプロセッサは、第2のデバイスから受信される少なくとも1つのメッセージの第3の信号強度を決定し、第3の信号強度データを、第1のデバイスへのサポートデータに含めるように構成されている。第1のメッセージプロセッサは、第2のデバイスから受信される少なくとも1つのメッセージの第1の信号強度を決定し、第1の信号強度及び第3の信号強度を、決定された距離におけるそれぞれの予測信号強度と比較することによって、決定された距離が信頼可能であるか否かを検証するように構成されている。この実施形態において、付加的に、信号強度に基づく距離測定が、信頼性を増大させるために実施される。到達時刻及び送信時刻に加えて、受信信号強度も、距離の測定値として使用することができる。デバイスは、メッセージを別のデバイスに送信する送信パワーを、そのメッセージに含め、この他のデバイスは、受信信号強度を測定し、他のデバイスは、仮定されているトランスミッタアンテナ特性(例えば、全方向性であること)、及び、信号強度が距離の2乗に反比例して低減することに基づいて、距離を決定することができる。少なくとも1つの協働デバイスがその同じメッセージの信号強度を測定し、そのようなデータを第1のデバイスに転送されるサポートデータに含めるとき、第1のデバイスは、受信信号強度に基づいて、第2のデバイスからの距離の比を決定する。

【0126】

一実施形態において、第1のデバイス及び第3のデバイスは、3GPPネットワーク内の基地局によって具現化され、一方、第2のデバイスはUEによって具現化される。3GPPにおける基地局は、いわゆるリソース要素の時間一周波数グリッドにおいて送受信する。時間一周波数グリッドにおける位置のいくつかは、3GPP規格によって固定されており、例えば、基地局が何かを特定のUEに(ダウンリンク)送信する時刻及び周波数、並びに、特定のUEが何かを基地局に(アップリンク)又は特定の他のUEに(サイドリンク)送信する時刻及び周波数の情報などのシステム情報を基地局の範囲内のすべてのUEにブロードキャストするために使用される。基地局が、本発明に従って協働しているとき、それらの時間一周波数グリッドは位置整合及び同期されるべきであり、それらは各々、グリッド内の同じ時間一周波数位置(リソース要素)を利用可能にすべきであり、そのため、それらはすべて、同じUEからの同じメッセージの到達時刻又は受信信号強度を測定することが可能である。

【0127】

さらなる実施形態において、測距プロトコルは、例えば、認証情報(例えば、公開鍵)又は認証情報若しくは暗号化認証情報のハッシュを含む、例えば、[802.11]において定義されているように測距プロトコルに追加される追加の属性又は追加のメッセージを含む。そのようなメッセージは、鍵データに基づいて暗号によって保護されているメッセージの一例である。第2のデバイスは、測距プロトコルのためのメッセージ交換の一部として、そのような認証情報又は認証情報若しくは暗号化認証情報のハッシュを含む。対称にするために、第1のデバイスも、そのような認証情報、認証情報若しくは暗号化認証情報のハッシュをさらなるメッセージに含める。測距プロトコルのメッセージ内に認証情報又は認証情報若しくは暗号化認証情報のハッシュを含める好ましいフィールドは、そのフィールドを転送する信号又は信号の少なくとも一部がメッセージの送信時刻又は到達時刻を測定するために使用されるフィールドであり、結果、別のデバイスがその認証情報又はその認証情報若しくはその暗号化認証情報を、第1のデバイスと第2のデバイスとの間の距離を測定されるために使用されるメッセージ内に挿入することは、不可能とは言わないまでも、非常に困難である。認証情報又は認証情報若しくは暗号化認証情報のハッシュを搬送する信号が、距離を測定するために使用される信号に(時間的に)近いほどよい。

このように、第1のデバイスは、測距プロトコルのメッセージ内の認証情報又は認証情報若しくは暗号化認証情報のハッシュが、実際に、距離測定プロトコルを交換している第2のデバイスのものであることを確信することができる。1つの実施形態において、第1のメッセージプロセッサは、この認証情報又は認証情報若しくは暗号化認証情報のハッシュを処理し、W i e f i（登録商標）保護セットアッププロトコル、デバイスプロビジョニングプロトコル、ディフィー・ヘルマン鍵交換及び／又は4ウェイW P A 2ハンドシェイクなどを使用することによって、これが、デバイス認証の実施及び相互信用の確立に成功したデバイスによって以前に使用された信用情報と一致するか否かを検証する。一致が見出された場合、第1のデバイスは、第1のデバイスと第2のデバイスとのあいだの距離測定を信用し、信頼可能と考えることができると仮定する。一致が見出されない場合、第1のデバイスは、第1のデバイスと第2のデバイスとの間の距離測定を信用せず、他の実施形態において説明されているようなメカニズムを使用するなど、距離測定の信頼性を検証する追加のステップを実施する。別の実施形態において、測定値（例えば、第1の時間データ及び／又は第2の時間データ）が、合意された、又は、第1のデバイスと第2のデバイスとの間で実施されている先行するデバイス認証手順中に確立されているものとしての第1のデバイスと第2のデバイスとの間の合意されている認証情報から導出される鍵を使用して暗号化される。

【0128】

代替的な実施形態において、第2のデバイスは、後の接続構成中に使用される、認証情報又は認証情報若しくは暗号化認証情報のハッシュを含む。第1のメッセージプロトコルは、測定されている距離を、認証情報によって接続する特定のデバイスと安全に相関付けるために、第1のデバイスと第2のデバイスとの間の測定されている距離とともに、認証情報又は認証情報若しくは暗号化認証情報のハッシュを処理及び記憶するように構成されている。第1のデバイスと第2のデバイスとの間の接続が構成されると、第1のデバイスは、同じ認証情報又はその派生物が、W i e f i（登録商標）保護セットアッププロトコル、デバイスプロビジョニングプロトコル、ディフィー・ヘルマン鍵交換の実施中及び／又は4ウェイW P A 2ハンドシェイクを実施している間など、デバイス認証を実施している間に使用されるか否かを検証する。そうすることによって、第1のデバイスは、接続しているデバイスが、特定の距離測定が行われたものと同じデバイスであると決定することができる。特に、認証情報が公開鍵であった場合、且つ、第1のデバイスと第2のデバイスとの間の接続の構成が、第2のデバイスが距離測定における認証情報として公開鍵に属する秘密鍵の所有権を有することをデバイス1に対して証明することに成功したことを含んでいた場合、第1のデバイスは、第2のデバイスがそこまでの距離を測定したものであり、詐称者でないと確信することができる。

【0129】

一実施形態において、第1のメッセージプロセッサは、決定された距離が信頼可能でないという評価を受けて、意図されているプロセスの代わりに、異なるプロセス又は機能、データ又は機能に対するアクセスの拒否に進むように構成されている。例えば、通常の距離に基づくプロセスは、位置に基づくサービス又はローカルな周辺機器にアクセスすることを許可することであり得る。また、例えば、イーサネット、インターネット、3 G P P基幹ネットワークなどの別のネットワークを介した第1のデバイスへの又は第1のデバイスからのルーティングが、距離測定に基づいて制御又は拒否される。決定された距離が信頼可能でないと考えられる場合、すべてのさらなる通信及び／又はアクセスが拒絶され、及び／又は、管理システム又は警備人員に警告メッセージが送信される。また、第1のメッセージプロセッサは、任意の通常の距離に基づくプロセスに進む前に、追加の認証情報及び／又はユーザの個人識別情報の要求などの異なるセキュリティプロトコルを第2のデバイスと関与させるように構成されている。異なるセキュリティプロトコルは、追加のプロセス又はメインプロトコルをさらに増強して実行することであってもよく、例えば、通常のセキュリティプロセスにおけるより厳重で厳密なステップをもたらす。任意選択的に、第1のメッセージプロセッサは、例えば、非常に近い距離にあるN F Cなど、異なる測

距プロトコル及び／又は異なるタイプの無線通信を使用して、又は、何らかの識別情報及び／又は指紋などの生体認証データを提供するために第2のデバイスの人間のオペレータによって、さらなる距離測定を要求するように構成されている。また、第1のメッセージプロセッサは、任意の通常の距離に基づくプロセスに進む前に、第1のデバイス内の少なくともいくつかのデータ及び／又は少なくとも1つのアプリケーションに対するアクセスを拒否又は制限するように構成されている。例えば、距離が信頼可能と考えられる場合に拡張サービスが提供される一方で、たとえ距離が信頼可能でないと考えられる場合であっても、基本サービスが提供される。

【0130】

図8は、第1のデバイスと第2のデバイスとの間の無線通信を介して距離を測定するための方法を示し、無線通信は、上述したような測距プロトコルを含む。第1のデバイス及び第2のデバイスは、図示され、図1を参照しながらさらに説明した第1のデバイス及び第2のデバイスと同様である。第3のデバイスが、第1のデバイスから信用される距離に位置する協働デバイスとして動作している。方法は、第1のデバイス内のプロセッサによって実行されるが、受信到達時刻及びサポートデータに基づいて、異なるデバイス内のプロセッサによって、及び／又は、異なる時点においても処理される。例えば、方法は、測距プロトコルに能動的に関与していないが、すべてのメッセージを受信し、信頼できる距離を認識しているさらなるデバイスにおいて実行される。

【0131】

方法は、ノードSTART（開始）801において開始する。第1の段階RNGP802において、方法は、図1を参照しながら説明したように、測距プロトコルを実行し、到達時刻測定を実施する。方法は、段階OD1803によって、第1のデバイスにおける測定メッセージの第1の到達時刻に基づいて第1のデバイスと第2のデバイスとの間の第1の距離を得ることによって継続し、その後、段階CO__COP804において協働デバイスと通信する。協働デバイスは、協働デバイスにおける測定メッセージの第3の到達時刻を決定し、サポートデータを提供するように構成されており、サポートデータは、第3の到達時刻に基づく。その後、方法は、決定された距離を評価することによって継続する。次の段階OD3805において、例えば、測定メッセージの第3の到達時刻及び送信時刻に基づいて計算されるサポートデータを使用して、第3のデバイスと第2のデバイスとの間の第3の距離が得られる。最後に、段階VERT806において、第1の距離、信用される距離及び第3の距離に関する検証テストが実施される。検証テストは、上記距離が、第1のデバイス、第2のデバイス及び協働デバイスの有効な空間的配置に対応するときに、第1の距離を信頼可能であるとして許容する。テストは、上記で明らかにされているように、三角不等式及び非一貫性チェックに基づく。

【0132】

一実施形態において、方法は、第1のデバイスが、第1の到達時刻又は第1の距離を提供するための開始デバイスとして動作するように命令される準備段階を含む。同様に、第3のデバイスが、第3の到達時刻に基づくサポートデータを提供するための協働デバイスとして動作するように命令される。準備段階は、別個の制御デバイス、コンピュータ又はサーバによって実行される。代替的に、第1のデバイス又は第3のデバイスが上記命令を実行してもよい。

【0133】

図9は、上記で図8によって説明したような第1のデバイスと第2のデバイスとの間の無線通信を介した距離測定において協働デバイスとして動作するための方法を示す。協働デバイスは、第1のデバイスから信用される距離に位置する。

【0134】

方法は、ノードSTART901において開始する。第1の段階RNGP902において、方法は、第1のデバイス及び第2のデバイスによって実施されるものとしての測距プロトコルを監視する。方法は、段階ARR3903によって、協働デバイスにおける測定メッセージの第3の到達時刻を決定することによって継続する。その後、段階CO__I

N 904において、協働側がその後、例えば、無線プロトコルを使用して、又は、有線接続を使用して、第1のデバイスと通信する。次に、段階SUP 905において、方法は、サポートデータを第1のデバイスに提供する。サポートデータは、第3の到達時刻に基づく。その後、方法は、協働側において、ノードEND（終了）906において終了する。上述したように、第1のデバイスは、サポートデータを使用して協働デバイスと第2のデバイスとの間の第3の距離を取得し、第1の距離、信用される距離及び第3の距離に関する検証テストを実施するように構成されている。

【0135】

図10aは、コンピュータプログラム1020を含む書き込み可能部分1010を有するコンピュータ可読媒体1000を示しており、コンピュータプログラム1020は、プロセッサシステムに、図9～図10を参照しながら説明したようなシステム内の上記方法のうちの1つ又は複数を実施させるための命令を含む。コンピュータプログラム1020は、コンピュータ可読媒体1000上で、物理マークとして、又は、コンピュータ可読媒体1000の磁化によって具現化される。しかしながら、任意の他の適切な実施形態もまた考えられる。さらに、コンピュータ可読媒体1000はここでは光ディスクとして示されているが、コンピュータ可読媒体1000は、ハードディスク、ソリッドステートメモリ、フラッシュメモリなどのような任意の適切なコンピュータ可読媒体であってもよく、記録不可能又は記録可能であってもよいことが理解されよう。コンピュータプログラム1020は、プロセッサシステムに、上記方法を実施させるための命令を含む。

【0136】

図10bは、図9～図10を参照しながら説明したようなデバイス又はサーバの一実施形態によるプロセッサシステム1100の概略図を示す。プロセッサシステムは、1つ又は複数の集積回路1110を含む。1つ又は複数の集積回路1110のアーキテクチャが、図に概略的に示されている。回路1110は、一実施形態による方法を実行し、及び／又は、そのモジュール若しくはユニットを実装するためにコンピュータプログラム構成要素を作動させるための処理ユニット1120、たとえば、CPU、を備える。回路1110は、プログラミングコード、データなどを記憶するためのメモリ1122を備える。メモリ1122の一部分は、読み出し専用であってもよい。回路1110は、通信要素1126、たとえば、アンテナ、コネクタ又はそれらの両方などを備える。回路1110は、方法において定義されている処理の一部分又はすべてを実施するための専用集積回路1124を備える。プロセッサ1120、メモリ1122、専用IC 1124及び通信要素1126は、相互接続部1130、たとえば、バス、を介して互いに接続される。プロセッサシステム1110は、それぞれアンテナ及び／又はコネクタを使用して、接触及び／又は非接触通信するように構成される。

【0137】

ネットワークからダウンロード可能であり、並びに／又は、コンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶されるコンピュータプログラム製品が提供され、製品は、下記にさらに明らかにされるように、位置情報を保護するために、コンピュータ上で実行されるときに、上記方法を実施するためのプログラムコード命令を含む。

【0138】

本発明による任意の方法は、プロセッサシステムに、それぞれの方法を実施させるための命令を含むソフトウェアを使用して実行される。ソフトウェアは、システムの特定のサブエンティティによって行われるステップのみを含んでもよい。ソフトウェアは、ハードディスク、フロッピー、メモリなどのような適切な記憶媒体内に記憶されてもよい。ソフトウェアは、ワイヤに沿って、又は無線で、又は、データネットワーク、例えば、インターネット、を介して、信号として送信されてもよい。ソフトウェアは、ダウンロード、及び／又は、サーバ上での遠隔使用のために利用可能とされる。本発明による方法は、プログラム可能論理、例えば、フィールドプログラマブルゲートアレイ（FPGA）を、本方法を実施するように構築するように構成されているビットストリームを使用して実行され

る。ソフトウェアが、ソースコード、オブジェクトコード、コード中間ソース、及び、部分的にコンパイルされた形態のようなオブジェクトコードの形態であってもよく、又は、本発明による方法を実施するのに使用するのに適した任意の他の形態であってもよいことが理解されよう。コンピュータプログラム製品に関する実施形態は、記載されている方法のうちの少なくとも1つの処理ステップの各々に対応するコンピュータ実行可能命令を含む。これらの命令は、サブルーチンに細分化され、及び／又は、静的に動的にリンクされる1つ若しくは複数のファイル内に記憶される。コンピュータプログラム製品に関する別の実施形態は、記載されているシステム及び／又は製品のうちの少なくとも1つの手段の各々に対応するコンピュータ実行可能命令を含む。

【0139】

明瞭にするために、上記の記載は、種々の機能ユニット及びプロセッサを参照しながら本発明の実施形態を説明していることが理解されよう。しかしながら、種々の機能ユニット又はプロセッサ間での機能の任意の適切な分布が、本発明から逸脱することなく使用される。例えば、別個のユニット、プロセッサ又はコントローラによって実施されるものとして示されている機能は、同じプロセッサ又はコントローラによって実施されてもよい。したがって、特定の機能ユニットに対する参照は、厳密な論理的又は物理的構造又は編成を示すのではなく、記載されている機能を提供するための適切な手段に対する参照と考えられるに過ぎない。本発明は、ハードウェア、ソフトウェア、ファームウェア又はこれらの任意の組み合わせを含む任意の適切な形態において実施することができる。

【0140】

本明細書において、「備える」という単語は、列挙されているもの以外の要素又はステップが存在することを除外するものではなく、要素が単数形の場合、これは、そのような要素が複数存在することを除外するものではないこと、任意の参照符号は、特許請求の範囲を限定するものではないこと、本発明はハードウェアとソフトウェアの両方によって実施されること、及び、いくつかの「手段」又は「ユニット」は、同じハードウェアアイテム又はソフトウェアアイテムによって表され、プロセッサが、場合によってハードウェア要素と協働して、1つ又は複数のユニットの機能を実現することに留意されたい。さらに、本発明は、上記実施形態に限定されず、本発明は、上記に記載されている又は相互に異なる従属請求項に列挙されているあらゆる新規の特徴又は特徴の組み合わせに存する。

【0141】

参考文献

[36.133] 3GPP TS 36.133: 「Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management」

[36.211] 3GPP TS 36.211: 「Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation」

[36.214] 3GPP TS 36.214: 「Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer - Measurements」

[36.321] 3GPP TS 36.321: 「3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification」

[36.355] 3GPP TS 36.355: 「Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)」

[37.571-1] 3GPP TS 37.571-1:「Universal Terrestrial Radio Access (UTRA) and Evolved UTRA (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification for UE positioning; Part 1: Conformance test specification」

[802.11] IEEE Computer Society「IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications」(IEEE Std. 802.11-2016)、December 2016

10

[802.1AS] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1AS: Timing and synchronization for time sensitive applications in bridged local area networks, Reference number ISO/IEC/IEEE 8802-1AS:2014 (E)

20

[DH] Diffie, W.; Hellman, M. (1976)「New directions in cryptography」IEEE Transactions on Information Theory, 22 (6): 644-654

[DPP] Device Provisioning Protocol - Technical Specification - Version 1.0, Wi-Fi (登録商標) Alliance, 2018, [https://www.Wi-Fi\(登録商標\).org/file-member/device-provisioning-protocol-specification](https://www.Wi-Fi(登録商標).org/file-member/device-provisioning-protocol-specification)

[NAN] Neighbor Awareness Networking - Technical Specification - Version 2.0, Wi-Fi (登録商標) Alliance, 2017, [https://www.Wi-Fi\(登録商標\).org/file-member/Wi-Fi\(登録商標\)-nan-technical-specification](https://www.Wi-Fi(登録商標).org/file-member/Wi-Fi(登録商標)-nan-technical-specification)

30

[OTDOA] Sven Fischer「Observed Time Difference Of Arrival (OTDOA) Positioning in 3GPP LTE」Qualcomm Technologies, Inc., June 6, 2014

[OWE] Opportunistic Wireless Encryption - Technical Specification - Version 1.0, Wi-Fi (登録商標) Alliance, 2018, [https://www.Wi-Fi\(登録商標\).org/file-member/opportunistic-wireless-encryption-specification](https://www.Wi-Fi(登録商標).org/file-member/opportunistic-wireless-encryption-specification)

40

【図面】

【図 1】

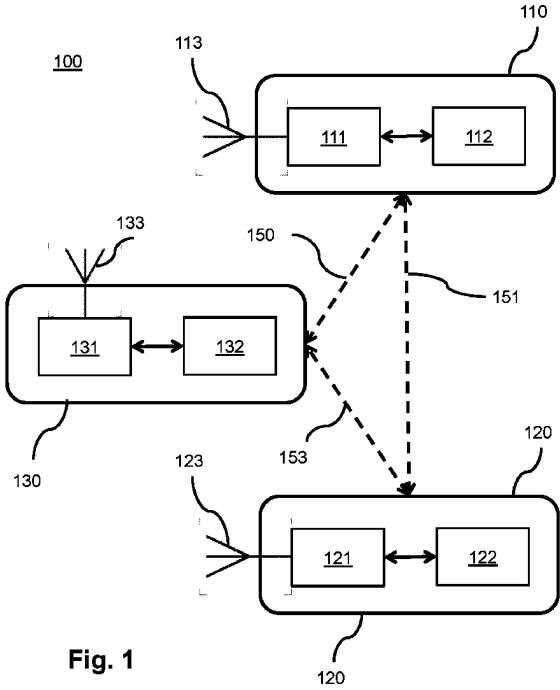


Fig. 1

【図 2】

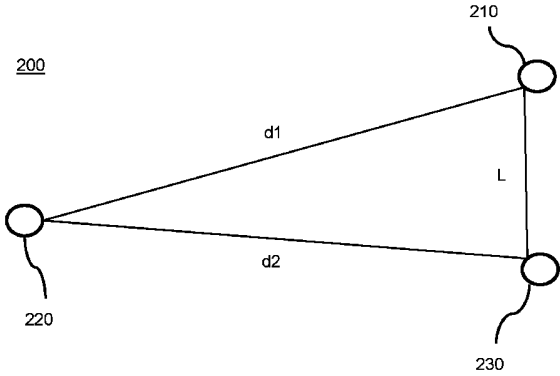


Fig. 2

【図 3】

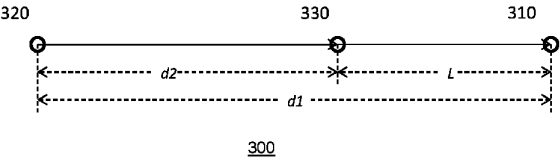


Fig. 3

【図 4】

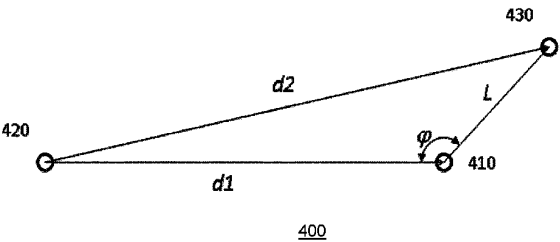


Fig. 4

【図 5】

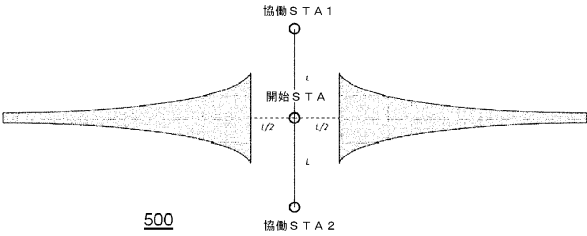


図 5

【図 6】

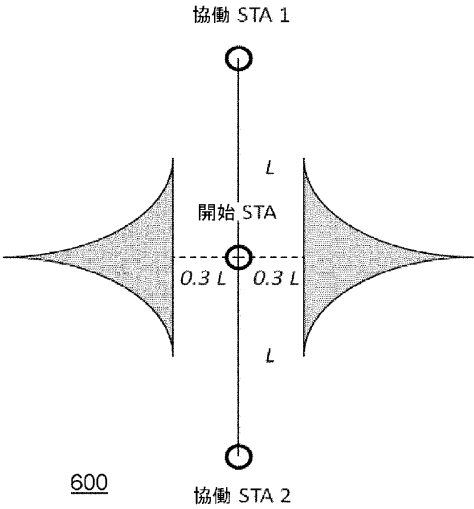


図 6

【図 7】

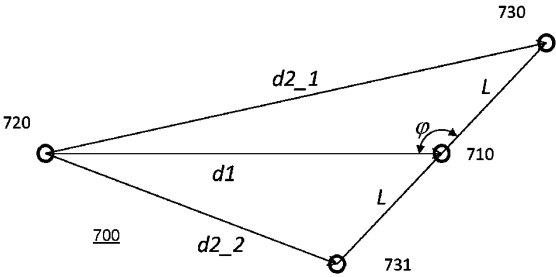


Fig. 7

【図 8】

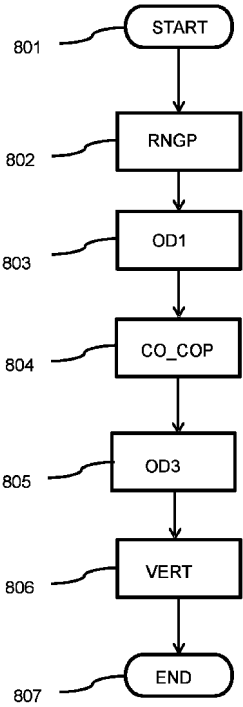


Fig. 8

10

20

30

40

50

【図 9】

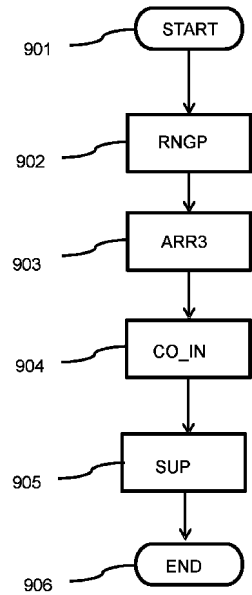


Fig. 9

【図 10 a】

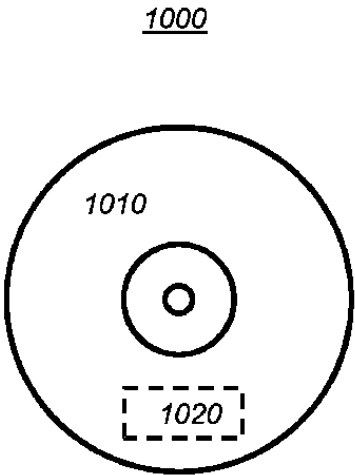


Fig. 10a

【図 10 b】

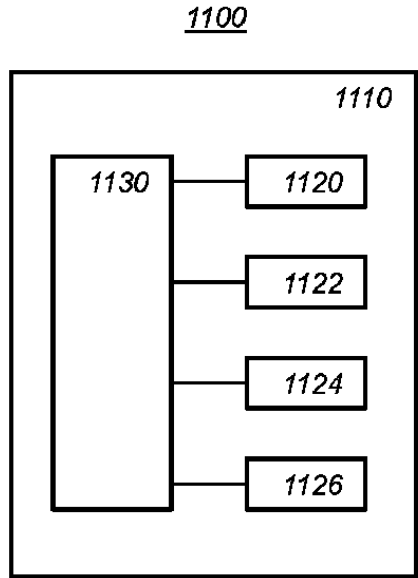


Fig. 10b

フロントページの続き

(51)国際特許分類	F I			
H 0 4 W	12/63	(2021.01)	H 0 4 W	12/63
H 0 4 W	64/00	(2009.01)	H 0 4 W	64/00 1 3 0

ドーフェン ハイ テック キャンパス 5

審査官 渡辺 慶人

(56)参考文献	特開 2 0 0 9 - 2 1 0 5 8 2 (J P , A)
	特表 2 0 1 9 - 5 0 3 4 7 2 (J P , A)
	特開 2 0 1 7 - 1 9 4 4 4 5 (J P , A)
	米国特許出願公開第 2 0 1 2 / 0 3 1 5 8 9 5 (U S , A 1)
	米国特許出願公開第 2 0 1 7 / 0 3 5 9 1 6 9 (U S , A 1)

(58)調査した分野	(Int.Cl., D B 名)
	G 0 1 S 5 / 0 0 - 5 / 3 0
	1 1 / 0 0 - 1 1 / 1 6
	1 9 / 0 0 - 1 9 / 5 5
	H 0 4 B 7 / 2 4 - 7 / 2 6
	H 0 4 W 4 / 0 0 - 9 9 / 0 0