(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6290890号
(P6290890)

(45)発行日　平成30年3月7日(2018.3.7)　(24)登録日　平成30年2月16日(2018.2.16)

(51)Int.Cl.		F I		
H04W 4/08	(2009.01)	H04W	4/08	
H04W 12/04	(2009.01)	H04W	12/04	
H04W 84/12	(2009.01)	H04W	84/12	
H04L 9/32	(2006.01)	H04L	9/00	675A

請求項の数 6　(全 20 頁)

(21)出願番号	特願2015-529020 (P2015-529020)
(86)(22)出願日	平成25年8月29日 (2013.8.29)
(65)公表番号	特表2015-534313 (P2015-534313A)
(43)公表日	平成27年11月26日 (2015.11.26)
(86)国際出願番号	PCT/EP2013/067868
(87)国際公開番号	WO2014/033199
(87)国際公開日	平成26年3月6日 (2014.3.6)
審査請求日	平成28年8月24日 (2016.8.24)
(31)優先権主張番号	12182285.2
(32)優先日	平成24年8月30日 (2012.8.30)
(33)優先権主張国	欧州特許庁 (EP)
(31)優先権主張番号	61/695,022
(32)優先日	平成24年8月30日 (2012.8.30)
(33)優先権主張国	米国 (US)

早期審査対象出願

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
KONINKLIJKE PHILIPS N. V.
オランダ国　5656　アーエー　アインドーフェン　ハイテック　キャンパス　5
High Tech Campus 5, NL-5656 AE Eindhoven
(74)代理人　100122769
弁理士　笛田　秀仙
(74)代理人　100145654
弁理士　矢ヶ部　喜行

最終頁に続く

(54)【発明の名称】無線装置のグループ中のペアリング

(57)【特許請求の範囲】

【請求項１】

無線装置のグループ及び携帯型装置を有する無線通信のためのシステムにおいて用いられる無線通信のためのホスト装置であって、当該システムは、各々の装置は他の装置とデータを無線で交換するための無線トランシーバを有し、

前記グループの第１無線装置は第１ホスト機能を提供し、前記グループの第２無線装置は第２ホスト機能を提供し、第１及び第２無線装置は同じ無線装置であるかまたは異なる無線装置であり、

無線装置の前記グループは、第１秘密データを共有し、第１秘密データに基づくそれぞれの第１セキュア接続を介して第１ホスト機能を提供する第１無線装置への無線通信のために設定され、

前記携帯型装置は、装置通信プロセッサを有し、当該装置通信プロセッサは、

第１秘密データと異なる第２秘密データに基づくペアリング手順を用いて第２ホスト機能を提供する第２無線装置との第２セキュア接続を設定し、

第２セキュア接続を介して第２指示を受信し、第２指示に従って、

第１秘密データと異なる第３秘密データに基づくそれぞれのペアリング手順を用いて前記グループの少なくとも１つの無線装置とのそれぞれの直接無線セキュア接続を設定し、

第２ホスト機能を提供する第２無線装置はホスト通信プロセッサを有し、当該ホスト通信プロセッサは、

第２秘密データに基づくペアリング手順を用いて前記携帯型装置との第２セキュア接続を

設定し、
前記携帯型装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第１指示であって、前記第３秘密データを有する第１指示を、第１セキュア接続を介して前記少なくとも１つの無線装置に転送し、
第３秘密データに基づいて前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第２指示を、第２セキュア接続を介して前記携帯型装置に転送し、
前記少なくとも１つの無線装置は通信プロセッサを有し、当該通信プロセッサは、
第１セキュア接続を介して第１指示を受信し、第１指示に従って、
第３秘密データに基づくそれぞれのペアリング手順を用いて前記携帯型装置とのそれぞれの直接無線セキュア接続を設定する、システムであり、前記ホスト装置は、
他の無線装置とデータを無線で交換するための無線トランシーバ、および
ホスト通信プロセッサを有し、当該ホスト通信プロセッサは、
第２秘密データに基づくペアリング手順を用いて前記携帯型装置との第２セキュア接続を設定し、
前記携帯型装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第１指示であって、前記第３秘密データを有する第１指示を、第１セキュア接続を介して少なくとも１つの無線装置に転送し、
第３秘密データに基づいて前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第２指示を、第２セキュア接続を介して前記携帯型装置に転送することにより、第２ホスト機能を提供し、
前記ホスト通信プロセッサが、前記携帯型装置へのそれぞれの直接無線セキュア接続を設定する前に第１セキュア接続を切断するために前記少なくとも１つの無線装置に第３指示を転送するように用意される、
ホスト装置。
【請求項２】
無線装置のグループ及び携帯型装置を有する無線通信のためのシステムにおいて用いられる無線通信のためのホスト装置であって、当該システムは、各々の装置は他の装置とデータを無線で交換するための無線トランシーバを有し、
前記グループの第１無線装置は第１ホスト機能を提供し、前記グループの第２無線装置は第２ホスト機能を提供し、第１及び第２無線装置は同じ無線装置であるかまたは異なる無線装置であり、
無線装置の前記グループは、第１秘密データを共有し、第１秘密データに基づくそれぞれの第１セキュア接続を介して第１ホスト機能を提供する第１無線装置への無線通信のために設定され、
前記携帯型装置は、装置通信プロセッサを有し、当該装置通信プロセッサは、
第１秘密データと異なる第２秘密データに基づくペアリング手順を用いて第２ホスト機能を提供する第２無線装置との第２セキュア接続を設定し、
第２セキュア接続を介して第２指示を受信し、第２指示に従って、
第１秘密データと異なる第３秘密データに基づくそれぞれのペアリング手順を用いて前記グループの少なくとも１つの無線装置とのそれぞれの直接無線セキュア接続を設定し、
第２ホスト機能を提供する第２無線装置はホスト通信プロセッサを有し、当該ホスト通信プロセッサは、
第２秘密データに基づくペアリング手順を用いて前記携帯型装置との第２セキュア接続を設定し、
前記携帯型装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第１指示であって、前記第３秘密データを有する第１指示を、第１セキュア接続を介して前記少なくとも１つの無線装置に転送し、
第３秘密データに基づいて前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第２指示を、第２セキュア接続を介して前記

携帯型装置に転送し、
前記少なくとも１つの無線装置は通信プロセッサを有し、当該通信プロセッサは、
第１セキュア接続を介して第１指示を受信し、第１指示に従って、
第３秘密データに基づくそれぞれのペアリング手順を用いて前記携帯型装置とのそれぞれの直接無線セキュア接続を設定する、システムであり、前記ホスト装置は、
他の無線装置とデータを無線で交換するための無線トランシーバ、および
ホスト通信プロセッサを有し、当該ホスト通信プロセッサは、
第２秘密データに基づくペアリング手順を用いて前記携帯型装置との第２セキュア接続を設定し、
前記携帯型装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第１指示であって、前記第３秘密データを有する第１指示を、第１セキュア接続を介して少なくとも１つの無線装置に転送し、
第３秘密データに基づいて前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第２指示を、第２セキュア接続を介して前記携帯型装置に転送することにより、第２ホスト機能を提供し、
前記ホスト装置は無線ドッキング・ホストまたは無線ドッキング・ステーションである、ホスト装置。
【請求項３】
前記ホスト通信プロセッサが、
第３秘密データを生成すること、
前記携帯型装置のそれぞれの異なるインスタンスのための第３秘密データのそれぞれの異なるセットを生成すること、
前記携帯型装置が、第２セキュア接続を切断した後に、第２セキュア接続をそれぞれ再度設定するときに、第３秘密データのそれぞれの異なるセットを生成すること、
無線装置のそれぞれの異なるサブセットのための第３秘密データのそれぞれの異なるセットを生成すること、および
第２秘密データに基づく若しくは第２秘密データに等しい第３秘密データを生成すること、
の少なくとも１つを行うように用意される、請求項１または請求項２に記載のホスト装置。
【請求項４】
前記ホスト通信プロセッサは、
第３秘密データに限られた寿命を指定すること、および／または
装置の認証レベルに応じて第３秘密データに寿命を指定すること、
を行うように用意される、請求項１から請求項３のいずれか一項に記載のホスト装置。
【請求項５】
無線装置のグループ及び携帯型装置を有する無線通信のためのシステムにおいて用いられる無線通信のための無線装置であって、当該システムは、各々の装置は他の装置とデータを無線で交換するための無線トランシーバを有し、
前記グループの第１無線装置は第１ホスト機能を提供し、前記グループの第２無線装置は第２ホスト機能を提供し、第１及び第２無線装置は同じ無線装置であるかまたは異なる無線装置であり、
無線装置の前記グループは、第１秘密データを共有し、第１秘密データに基づくそれぞれの第１セキュア接続を介して第１ホスト機能を提供する第１無線装置への無線通信のために設定され、
前記携帯型装置は、装置通信プロセッサを有し、当該装置通信プロセッサは、
第１秘密データと異なる第２秘密データに基づくペアリング手順を用いて第２ホスト機能を提供する第２無線装置との第２セキュア接続を設定し、
第２セキュア接続を介して第２指示を受信し、第２指示に従って、
第１秘密データと異なる第３秘密データに基づくそれぞれのペアリング手順を用いて前記

グループの少なくとも１つの無線装置とのそれぞれの直接無線セキュア接続を設定し、
第２ホスト機能を提供する第２無線装置はホスト通信プロセッサを有し、当該ホスト通信プロセッサは、
第２秘密データに基づくペアリング手順を用いて前記携帯型装置との第２セキュア接続を設定し、
前記携帯型装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第１指示であって、前記第３秘密データを有する第１指示を、第１セキュア接続を介して前記少なくとも１つの無線装置に転送し、
第３秘密データに基づいて前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを用いるための第２指示を、第２セキュア接続を介して前記携帯型装置に転送し、
前記少なくとも１つの無線装置は通信プロセッサを有し、当該通信プロセッサは、
第１セキュア接続を介して第１指示を受信し、第１指示に従って、
第３秘密データに基づくそれぞれのペアリング手順を用いて前記携帯型装置とのそれぞれの直接無線セキュア接続を設定する、システムであり、前記無線装置は、
前記携帯型装置並びに前記第１及び第２無線装置とデータを無線で交換するための無線トランシーバ、および
通信プロセッサを有し、当該通信プロセッサは、
第１セキュア接続を介して、第３秘密データを有する第１指示を受信し、第１指示に従って、
前記第３秘密データに基づくペアリング手順を用いて前記携帯型装置との直接無線セキュア接続を設定し、
前記通信プロセッサは、
前記携帯型装置へのそれぞれの直接無線セキュア接続を設定する前にそれぞれの第１セキュア接続を切断すること、および
前記携帯型装置へのそれぞれの直接無線セキュア接続を切断した後にそれぞれの第１セキュア接続を復元すること、
の少なくとも１つを行うように用意される、
無線装置。

【請求項６】

前記通信プロセッサは、前記携帯型装置へのそれぞれの直接無線セキュア接続の設定を開始するように用意される、請求項５に記載の無線装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、無線装置及び携帯型装置のグループを含む無線通信のシステムに関し、各々の装置は、他の装置と無線でデータを交換するための無線トランシーバを含み、グループの第１無線装置は第１ホスト機能を提供し、グループの第２無線装置は第２ホスト機能を提供し、第１及び第２無線装置は、同じ無線装置であるか異なる無線装置であり、無線装置のグループは第１秘密データを共有し、第１秘密データに基づくそれぞれの第１セキュア接続を介して第１ホスト機能を提供する第１無線装置への無線通信のために設定される。

【０００２】

本発明はさらに、無線通信のための上記のシステム用の、携帯型装置、ホスト装置、無線装置、方法及びコンピュータ・プログラムに関する。

【０００３】

本発明は、例えばWi-Fiを介したセキュアな無線通信の分野に関し、より具体的には、無線ドッキング・システムのためのセキュアな設定に関する。

【背景技術】

【０００４】

例えばIEEE 802.11文献から知られるWi-Fiのような、無線通信において、装置は、セキュアな接続を構成するために、例えばwww.wi-fi.orgから入手可能な"Wi-Fi Protected Access (WPA), Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August, 2004, by the Wi-Fi Alliance"に記述されるように、ペアを組まれる必要がある。本発明はWi-Fiシステムを用いてさらに説明されるが、本発明が同様に他の無線通信システム（例えばBluetooth：BLUETOOTH SPECIFICATION, Core Package version 2.1 + EDR, 2007年7月26日発行参照）に適用されることができることに留意されるべきである

【０００５】

Wi-Fi接続は、WPA2のような技術を用いる暗号手段によって守秘性及び整合性のために保護される。WPA2におけるセキュリティは、2つのシステムに基づくことができる。第１のシステムは、事前共有キー・モード（PSK：パーソナル・モードとしても知られる）であり、家庭及び小規模オフィス・ネットワークのために設計される。第２のシステムは、802.1X認証サーバの使用に依存し、企業ネットワークのために設計される。

【０００６】

PSKモードでは、互いに通信する全ての装置は256ビット・キーを共有し、それは『パスフレーズ』と呼ばれる。同様にWi-Fi Allianceからの文献"Wi-Fi Simple Configuration, Technical Specification, Version 2.0.2, 2011"から知られるWi-Fi Simple Configuration（別名、Wi-Fi保護セットアップ）は、パスフレーズを知る第1装置（例えば無線LANアクセス・ポイント）が、それを、ユーザが第2装置においてパスフレーズを入力することを必要とせずに、セキュアな方法で、第2装置に送信することを可能にする規格である。その代わりに、ユーザは、パスフレーズを受信するために、例えば制限された時間内に両方の装置のボタンを押すか、または第１装置にリストされる8桁のPINを第２装置に入力することができる。これは、一般的にユーザの動作（すなわち、いわゆるユーザ・ペアリング動作）を必要とする。

【０００７】

US2010/0153727は、共通のノンスを生成するために用いられるノンスを交換する、複数の無線装置の間の直接リンク通信のための拡張セキュリティを記述する。グループ識別情報要素は、少なくとも共通ノンスから生成されて、認証サーバに転送される。認証サーバは、キー同意グループの一部として装置を照合するために、グループ識別情報要素から、グループ直接リンク・マスターキーを生成する。グループ・キーも、共通ノンスに基づいて生成される。こうして、直接リンク通信のための装置のセキュアなグループが生成される。

【０００８】

Wi-Fiインフラストラクチャにおいて、アクセス・ポイント(AP)、厳密にはそのレジストラ(Registrar)は、それが責任を負うネットワークのための証明書を記憶及び管理する。あるAPのWi-Fiインフラストラクチャ・ネットワークへのアクセスを望むWi-Fi装置は、そのAPとのペアリング動作においてネットワーク証明書を取得する必要がある。一旦、APとのセキュアな接続が設定されると、Wi-Fi装置はそのAPと関連付けられた他のWi-Fi装置と通信することができる。従来のインフラストラクチャは、全ての通信がアクセス・ポイントを通過する必要があるので、接続が間接的であるという短所を有する。しかしながら、多くの場合において、装置が、アクセス・ポイントを通してトラフィックを中継することを要せずに、互いの間の直接リンクを設定することが可能であることは、(例えば、待ち時間低減、接続速度改善のために)有益である。装置間のそのような直接Wi-Fiリンクを設定することを可能にするために、２つの技術、Wi-Fi Direct及びTunneled Direct Link Setup(TDLS)が開発された。

【０００９】

同様にWi-Fi Allianceからの"Wi-Fi Wi-Fi Peer-to-Peer (P2P) Technical Specification, Version 1.1, 2010"から知られるWi-Fi Direct（別名、Wi-Fiピア・ツー・ピア）は、Wi-Fi装置が無線アクセス・ポイントを必要とせずに互いに接続することを可能にする

規格である。Wi-Fi Directは、表示装置/Wi-Fiディスプレイをサポートする周辺機器、及び入出力装置/ Wi-Fiシリアル・バスをサポートする周辺機器（例えば、無線マウス、キーボード、プリンタ、USBハブ）のような、スタンドアロンの無線装置及び周辺機器を接続するための重要な役割を果たす。したがって、それは、無線ドッキングのための重要な技術、携帯型装置が多数の無線周辺機器に接続することを可能にする技術である。Wi-Fi Directにおいて、ユーザ・ペアリング・ステップは、一般的に、生成される新たなWi-Fi Direct接続ごとに実行される必要がある。2つのWi-Fi Direct装置が通信することを望むときに、それらのうちの一方はいわゆるグループ・オーナー(GO)になる。他方の装置は、クライアントの役割を担う。合わせて、それらは、いわゆるP2Pグループを形成する。GOは、APと多くの類似性を有する。それは、例えば、他の装置がP2Pグループに参加することを可能にし、P2Pグループ中の異なる装置間でトラフィックを配信することを可能にする。しかしながら、上述のように、トラフィックを中継することを要せずに、装置が互いに直接通信することが可能であることは有益である。Wi-Fi Directの場合、これは、個別に他の装置の各々と接続してペアリングしならなければならないことを意味する。これは、特に複数の装置が関与する場合にわずらわしい。例えば、多数の無線周辺機器との携帯型装置の無線ドッキングのために、ユーザが個別に各々の無線周辺機器とのユーザ・ペアリング・ステップを実行することを必要とする場合、ユーザにとって非常に不親切である。したがって、ペアリング動作の量を最小限に保つことは非常に重要である。

【００１０】

文献"IEEE Std 802.11z-2010 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 7: Extensions to Direct-Link Setup (DLS), published by IEEE on 14 October 2010"から知られるTunneled Direct Link Setup(TDLS)は、Wi-Fiにおけるオプションであり、セキュアな直接接続を設定するために再びペアリングすることを必要とせずに、同じWi-Fiアクセス・ポイントにともに接続される2つの装置間の直接リンクを設定することを可能にする。これは以下のように実行される。一旦TDLS対応Wi-Fi装置がAPに接続されると、それは、直接接続を設定するために同じAPに接続される他のTDLS対応装置にリクエストを送ることができる。セキュリティ証明書及びどのWi-Fiチャネルを使用するかに関する情報のような情報を交換した後、2つの装置は、2つの装置間の専用のセキュアな直接リンクを開始することができる。

【００１１】

しかしながら、TDLSは、いくつかの欠点を有する。

【００１２】

関連する全ての装置は、(2つの異なる周波数上で動作することを含む、他の装置に対する直接リンク及びAPに対するリンクを同時に維持するために)同時並行の動作をサポートする必要があり、一方、多くの携帯型及び無線周辺機器は、１つのWi-Fi接続および/または１つの周波数Wi-Fi接続のみを設定して維持することが可能である。

【００１３】

TDLSは、Wi-Fi Directネットワークにおいて用いられるときに、いくつかの互換性問題を有する（例えば、Wi-Fi Direct P2Pグループ内で異なる装置間の直接リンクを設定するWi-Fi Direct GOを通したTDLS)。例えば、Wi-Fi Direct及びTDLSのパワー節約メカニズムは、互換性がなく、競合を引き起こすこと場合がある。

【００１４】

TDLS直接リンクのためのセキュリティ証明書の交換は、TDLSピア・キー(TPK)ハンドシェイクで実行される。問題は、2つのTDLS装置間のこのハンドシェイクがAPを介して実行されることである。APは、関連するTDLS装置のメッセージを解読することができるので、APは、このハンドシェイクを耳にすることができ、TDLS装置が直接接続のために同意するキーを回復することをできる。PSKモードが用いられるときに、同じAPに関連付けられた他の装置は、例えば以下のように、このトラフィックを耳にすることが可能である。Wi-Fi装置は、PSKを用いてAPと関連づけられるときに、それは、ペアワイズ一時キー(Pairwise Transient Key：PTK)と呼ばれるリンク・キーを生成/導出するために、いわゆる4ウェ

イ・ハンドシェイクにおいてパスフレーズ及び他の情報を用いる。PTKは、そのWi-Fi装置とAPとの間のトラフィックの暗号化及び認証のために用いられる。他の装置のためのトラフィックは、AP及び他の装置がパスフレーズから導き出したリンク・キー(PTK)でAPによって再暗号化される。APは各々の関連するWi-Fi装置のための異なるPTKを有するが、APと関連付けられた如何なる装置も、パスフレーズを所有し、他の装置とAPとの間の４ウェイ・ハンドシェイクをリスンすることによって、用いられているPTKを計算することができる。このPTKを用いることにより、装置は、他の装置とAPとの間の通信を解読することができるので、これは、それがTDLSピア・キー・ハンドシェイクを耳にすることができ、2つのTDLS装置間のTDLS直接リンクを保護するために用いられるキーを計算することができることを意味する。したがって、TDLSは、デフォルトでは、直接リンク上でのセキュアな専用通信を提供しない。

【００１５】

無線装置のペアリング及び接続設定は、常に、グループ中の全ての装置が接続される必要があるアクセス・ポイントを通して行われなければならない。最初にアクセス・ポイント/グループ・オーナーとの接続を設定しない限り、グループ中のクライアント/ステーション(例えばディスプレイ)のいずれとも直接接続することができない。これは、グループ中の他の装置のうちの１つを通してグループと接続することができないので、ペアリング・ステップを実行するためにアクセス・ポイント/グループ・オーナーに物理的に近いことを必要とする場合があることを意味する。

【発明の概要】

【発明が解決しようとする課題】

【００１６】

ユーザ・ペアリング・ステップの数を最小限に維持し、装置間の直接リンクの盗聴を防止し、グループに接続する際の柔軟性を提供するセキュアな通信のためのシステムを提供することが本発明の目的である。

【課題を解決するための手段】

【００１７】

この目的のために、冒頭の段落に記載される無線通信のためのシステムにおいて、携帯型装置は、第１秘密データと異なる第２秘密データに基づくペアリング手順を用いて第２ホスト機能を提供する第２無線装置との第２セキュア接続を設定し、第２セキュア接続を介して第２命令を受信し、第２命令に従って、第１秘密データと異なる第３秘密データに基づくそれぞれのペアリング手順を用いてグループのうちの少なくとも１つの無線装置とのそれぞれの直接無線セキュア接続を設定するための、装置通信プロセッサを有し、第２ホスト機能を提供する第２無線装置は、第２秘密データに基づくペアリング手順を用いて携帯型装置との第２セキュア接続を設定し、携帯型装置との直接無線セキュア接続を設定するために第３秘密データを適用するための第１命令を第１セキュア接続を介して前記少なくとも１つの無線装置へ転送し、第３秘密データに基づく前記少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを適用するための第２命令を第２セキュア接続を介して携帯型装置へ転送するための、ホスト通信プロセッサを有し、前記少なくとも１つの無線装置は、第１セキュア接続を介して第１命令を受信し、第１命令にしたがって、第３秘密データに基づくそれぞれのペアリング手順を用いて携帯型装置とのそれぞれの直接無線セキュア接続を設定するための、通信プロセッサを有する。

【００１８】

この目的のために、本発明のさらに別の態様では、冒頭の段落に記述される無線装置のシステムにおける無線通信方法は、第１秘密データと異なる第２秘密データに基づくペアリング手順を用いて第２ホスト機能を提供する第２無線装置と携帯型装置との間の第２セキュア接続を設定し、携帯型装置との直接無線セキュア接続を設定するために第１秘密データ(240)と異なる第３秘密データを適用するための第１命令を第１セキュア接続を介してグループのうちの少なくとも１つの無線装置に転送し、第３秘密データに基づく少なくとも１つの無線装置との直接無線セキュア接続を設定するために第３秘密データを適用す

るための第２命令を第２セキュア接続を介して携帯型装置へ転送し、第３秘密データに基づくそれぞれのペアリング手順を用いて携帯型装置と少なくとも１つの無線装置との間のそれぞれの直接無線セキュア接続を設定する。

【００１９】

セキュア・システム及び方法の主要な要素は、(例えばWi-Fi Direct互換の)携帯型装置Aが、無線装置のグループGに接続することを可能にする。グループGは、第１ホスト機能を提供する無線装置に接続されるグループとして動作するように予め設定され、グループの内の通信を安全にするために用いられる共通秘密S1を共有する。グループは、無線ドッキング・ホスト及び無線周辺機器を例えば有することができる。装置Aは、第２セキュア接続を介して通信を安全にするための秘密S2を用いてグループ中の、第２ホスト機能を提供することによって第２ホスト装置として機能する、無線装置のうちの1つに接続する。続いて、グループ中の装置及び装置Aは他の秘密S3について指示を受け、続いて、装置Aは、入力接続に対するリスンを開始し、１つ以上の装置は、装置Aとの自動化されたペアリングのために、例えばWi-Fi Directと互換性ある態様で、秘密S3を用いて装置Aとの直接セキュア無線接続を設定する。オプションとして、第２ホスト装置は、第１ホスト機能を提供する無線装置と同じ装置である。それゆえに、第１及び第２ホスト機能は、１つの無線装置において実施されることができる。さらに、グループGは、P2Pクライアントまたは Wi-Fiステーション(STA)の役割しかサポートすることができず、P2Pグループ・オーナーまたはWi-Fiアクセス・ポイント(AP)の役割をサポートすることができない装置を含むことができる。

【００２０】

これらの方策は、装置間の直接リンクの盗聴を防止し、第２ホストの機能を実行することが可能な任意の装置が、ある機能を実行する無線装置のグループに対するエントリーポイントであることを可能にすることによって、追加の柔軟性をさらに与える態様において、最小限のユーザ・ペアリング・ステップによりセキュアな直接リンクを設定するために使用される秘密を配信するための無線セキュア通信システム及びセキュア・プロトコルが提供されるという効果を有する。例えば、装置のグループは、スマートフォンのような携帯型装置のためのドッキング環境(別名、ドッキー（dockee）)を提供することができる。特に、dockeeは、グループと接続するためにドッキング・システム中の同じ装置(例えばAPまたはGO)を必ずしも用いる必要はなく、その代わりに、前記第２ホスト機能を提供するグループ中の任意の装置に接続することができる。

【００２１】

本発明はさらに、以下の認識に基づく(一例としてWi-Fi環境を用いる)。Wi-Fi Direct装置のグループが一緒に他の無線装置のための機能(例えば無線ドッキング)を実行するときに、この他の無線装置が、個別にグループからのこれらの装置の各々とのユーザ・ペアリング動作を実行することを要せずにグループ中の無線装置のいずれかとの１つ以上のピア・ツー・ピア・リンクを設定することをできることが望ましい。

【００２２】

Wi-Fi Directは、グループ・オーナー(GO)のコンセプトを有する。グループ中の全てのWi-Fi Direct装置が同じGOに接続し、GOがWi-Fi DirectのいわゆるIntra-BSS分配機能をサポートする場合、グループ中の全ての装置と通信することを可能にするためには、この他の無線装置がこのGOに接続すれば十分である。Intra-BSS Distributionフィールドは、P2P装置が、P2Pグループ中のクライアント間のデータ分配サービスを提供するP2Pグループをホストしているか、または、ホストすることを意図しているかを示す。しかしながら、全ての通信はGOを通らなければならない。これは、非常に非効率的であり、通信の待ち時間を増加させる。無線ドッキングのような機能のためには、待ち時間は重要な問題である。無線ディスプレイ、マウス、キーボード等との接続は、可能な限り待ち時間が短い必要がある。したがって、グループの複数の又は全てのメンバーとの直接(すなわちピア・ツー・ピア)接続を設定することが可能であることが重要である。しかしながら、それは、この周辺機器のグループに接続することを望む無線ドッキーごとに実行されるべき多数

のユーザ・ペアリング・ステップを要する。前のセクションにおいて言及された理由のために、TDLSを用いることは、この問題を解決するための選択肢ではない。

【００２３】

他の問題は、Wi-Fi Directが、特定の制限(例えばP2P装置は１つのGOにしか接続されることができないという制限)を装置に課すことである。一旦GOに接続されると、P2P装置は役割を変化させ、すなわち、装置はP2Pクライアントになる。Wi-Fi Directは、P2Pクライアントに対するさまざまな制限（例えば、P2Pクライアント間の発見可能性及び通信に関する制限）を定める。さらに、一般的に１つの装置上で動作することができる同時P2Pクライアント・インスタンスの数は、非常に制限される。多くのローエンドの無線周辺機器(例えばWi-Fiマウスまたはキーボード)は、それらのリソース制限に起因して更なる制限があることが予想される（例えば、P2Pクライアントの役割のみをサポートして、１つのWi-Fiリンクのみをサポートすること）。

【００２４】

本発明者らは、上記の問題は、第２ホストを介して、第３秘密データを生成して、グループの携帯型装置(ドッキー)及び無線装置に、グループの選択された無線装置に第１装置を接続するために（例えば予め設定されたドッキング環境を構成するために）、第３秘密データを適用するように指示するセキュア・プロトコルによって克服されることを認識した。

【００２５】

オプションとして、携帯型装置において、装置通信プロセッサは、グループ・オーナーとして前記直接無線接続を介して通信を制御するように、さらに用意される。無線ネットワークシステムでは一般に、装置は、例えばAPの役割を実行しているWLANにおける、グループ・オーナーとして装置のグループを制御することができる。Wi-Fiの実施例では、更なる無線装置のサブセットG'中の装置と第１装置との間のWi-Fi Direct P2P接続を設定するときに、第１装置はWi-Fi Directグループ・オーナーの役割を担う。

【００２６】

オプションとして、携帯型装置において、装置通信プロセッサは、それぞれの異なる第３秘密データに基づくそれぞれのペアリング手順を用いてそれぞれの異なるサブセットのそれぞれの無線装置とのそれぞれの異なる直接無線セキュア接続を設定するようにさらに用意される。長所として、複数のサブセットは、第３秘密データの異なるインスタンスを介して第１装置と通信するように適応される。

【００２７】

オプションとして、携帯型装置において、装置通信プロセッサは、複数のサブセットのためのそれぞれの異なる第３秘密データを含む第２命令を受信するようにさらに用意される。長所として、複数のサブセットは、一つの命令を介して携帯型装置と通信するように対応される。

【００２８】

オプションとして、携帯型装置において、装置通信プロセッサは、第３秘密データを生成して、第２ホスト機能を提供する装置に第３秘密データを転送するようにさらに用意される。長所として、携帯型装置は、第３秘密データの生成を制御することによって、セキュリティを制御する。

【００２９】

オプションとして、携帯型装置において、装置通信プロセッサは、サブセットのそれぞれの無線装置とのそれぞれの直接無線セキュア接続の設定を開始する前に第２セキュア接続を切断するように用意される。長所として、より少ない無線トランシーバ能力が必要とされ、より少ない容量の無線媒体が用いられる。

【００３０】

オプションとして、携帯型装置において、装置通信プロセッサは、永続的なグループ化を提供するように、そしてしかるべく、前記第３秘密データに基づくそれぞれの直接無線セキュア接続を切断した後に、再び前記第３秘密データに基づく更なるそれぞれの直接無

線セキュア接続を設定するように用意される。長所として、携帯型装置(例えばドッキー)が再接続するときに、セキュア通信がより高速で復元される。

【００３１】

オプションとして、携帯型装置において、装置通信プロセッサは、前記第３秘密データに基づくそれぞれの直接無線セキュア接続を切断した後に、それぞれの直接無線セキュア接続を設定するためにサブセットのそれぞれの無線装置と再接続するときに、以前のペアリングの間に取得された第２秘密データまたは第３秘密データを用いるように用意される。長所として、携帯型装置(例えばドッキー)が再接続するときに、セキュア通信がより高速で復元される。

【００３２】

オプションとして、第２セキュア接続は、Wi-Fi Direct P2P接続を含む。実際には、接続は、Wi-Fi Direct P2P接続であることができ、第２秘密データ(S2)は、Wi-Fiパスフレーズ(例えばWi-Fiペアワイズ・マスター・キー(PMK)またはWi-Fi事前共有キー(PSK))である。

【００３３】

オプションとして、それぞれの直接無線セキュア接続は、Wi-Fi Directピア・ツー・ピア接続を含み、および／または、それぞれの直接無線セキュア接続は、Tunneled Direct Link Setup(TDLS)接続を含む。実際には、サブセットG'中の装置と第１装置との間の直接接続は、Wi-Fi Direct P2P接続である場合があり、第３秘密データは、Wi-Fiパスフレーズ、例えばWi-Fiペアワイズ・マスター・キー(PMK)またはWi-Fi事前共有キー(PSK)である。別の態様では、サブセットG'中の装置と第１の装置との間の直接接続は、TDLS接続である。さらに、ペアリング手順は、Wi-Fi保護アクセス（Protected Access）(WPA/WPA2)またはWi-Fi Simple Configuration手順を有することができる。長所として、そのような既知のペアリング手順は、無線装置においてすでに利用可能であり、共有されていることができる。

【００３４】

オプションとして、事前構成ステップは、第２ホスト機能を提供する装置を、第２ホスト装置及びグループG中の装置から成るP2PグループのWi-Fi Direct P2Pグループ・オーナーとして指定すること、並びに、第２ホスト装置から共通秘密S1を得るために第２ホスト装置とグループ中の装置の各々とをペアリングすることを含み、S1はパスフレーズ(Wi-Fiペアワイズ・マスター・キー(PMK)またはWi-Fi事前共有キー(PSK))である。

【００３５】

オプションとして、ホスト装置において、ホスト通信プロセッサは、第３秘密データを生成するように用意される。長所として、ホスト装置は、第３秘密データの生成を制御することによって、セキュリティを制御する。

【００３６】

オプションとして、ホスト装置において、ホスト通信プロセッサは、第１装置のそれぞれの異なるインスタンスのための第３秘密データのそれぞれの異なるセットを生成するように用意される。長所として、通信の漏話は、異なる第１装置間で防止される。

【００３７】

オプションとして、ホスト装置において、ホスト通信プロセッサは、装置（A）が、第2セキュア接続を切断した後に、それぞれのさらなる時間に、第２セキュア接続を設定するときに、第３秘密データのそれぞれの異なるセットを生成するように用意される。長所として、第３秘密データの異なるセットを生成することによってリプレー攻撃が回避される。

【００３８】

オプションとして、ホスト装置において、ホスト通信プロセッサは、グループ中の無線装置のそれぞれの異なるサブセットのための第３秘密データのそれぞれの異なるセットを生成するように用意される。長所として、複数のサブセットが、第３秘密データの異なるインスタンスを介して第１装置と通信するために提供される。

【００３９】
オプションとして、ホスト装置において、ホスト通信プロセッサは、第２秘密データに基づくまたは等しい第３秘密データを生成するように用意される。基本的に、第３秘密データは第２秘密データと異なるように選択されることができ、それによってセキュリティを改善する。長所として、第３秘密データは第２秘密データに基づいて生成されることができ、それにより効率を改善する。さらに、第３秘密データは第２秘密データに等しいように選択されることができ、それにより、より少ないデータが転送される必要があるので、速度を改善する。
【００４０】
オプションとして、ホスト装置において、ホスト通信プロセッサは、限られた寿命を第３秘密データに割り当て、および/または、装置(A)のアクセス権限レベルに応じて第３秘密データに寿命を割り当てるように用意される。長所として、セキュア・システムに対するアクセスは時間的に制限され、または、ゲストもしくはオーナーは異なる権利を割り当てられることができる。
【００４１】
オプションとして、ホスト装置において、ホスト通信プロセッサは、装置にそれぞれの直接無線セキュア接続を設定する前に第１セキュア接続を切断するためにサブセットのそれぞれの無線装置へ第３命令を転送するように用意される。長所として、より少ない無線トランシーバ能力が必要とされ、より少ない容量の無線媒体が用いられる。
【００４２】
オプションとして、ホスト装置は、無線ドッキング・ホストまたは無線ドッキング・ステーションである。実際には、ホスト装置は、第１の無線ホスト装置および/または第２無線ホスト装置と同じ装置であることができる。それゆえに、第１及び第２ホスト機能は、１つのドッキング・ホストまたは無線ドッキング・ステーションにおいて実施されることができる。
【００４３】
オプションとして、無線装置において、それぞれの通信プロセッサは、携帯型装置に対するそれぞれの直接無線セキュア接続の設定を開始するように用意される。長所として、無線装置は、設定を制御する。
【００４４】
オプションとして、無線装置において、それぞれの通信プロセッサは、携帯型装置に対するそれぞれの直接無線セキュア接続を設定する前に第１セキュア接続を切断するように用意される。長所として、より少ない無線トランシーバ能力が必要とされ、より少ない容量の無線媒体が用いられる。
【００４５】
オプションとして、無線装置において、それぞれの通信プロセッサは、携帯型装置に対するそれぞれの直接無線セキュア接続を切断した後に第１セキュア接続を復元するように用意される。長所として、第１装置が切断された後で、予め設定されたグループは自動的に再接続される。
【００４６】
オプションとして、ホスト装置は、2つの独立したWi-Fi Direct P2Pグループ（一方のグループはグループGの装置から成り、一方はホスト装置とのP2P接続を有する携帯型装置から成る）の一部であることが可能である。
【００４７】
オプションとして、ホスト装置は、携帯型装置Aが接続する前にグループG中の他の装置に秘密S3を通知する。長所として、グループに対する携帯型装置の接続(例えばドッキング手順)は、より高速で完遂される。
【００４８】
オプションとして、ホスト装置は、Wi-Fi Direct継続グループ（Persistent Group）動作をサポートする。オプションとして、ホスト装置は、Wi-Fi Direct P2P Invitation手

順を用いてホスト装置に接続するように、グループGに装置を招待する。オプションとして、自動化されたペアリング手順は、Wi-Fi保護アクセス（Protected Access）に基づく(例えばWPAまたはWPA2)。オプションとして、自動化されたペアリング手順は、Wi-Fi Simple Configurationに基づく。オプションとして、携帯型装置は、バックボーンを必要とせずに、グループG中の無線装置が一緒に機能を実行するために互いに依然として通信することができるように、Wi-Fi Direct BSS内配信をサポートする。オプションとして、携帯型装置は、Wi-Fi Direct継続グループ化（Persistent Grouping）動作をサポートして、以降の接続においてサブセットG'の装置に接続するために第２ホスト装置を通したグループへの第１の接続の間に読み出される第３秘密データを用いる。長所として、そのようなオプションは、Wi-Fi対応装置の既存の要素の拡張である。

【００４９】

本発明による装置及び方法の更なる好ましい実施の形態は特許請求の範囲において与えられて、その開示は参照として本願明細書に組み込まれる。

【００５０】

本発明のこれらの及び他の態様は、添付の図面を参照して、一例として記述される実施の形態から明らかであり、それらを参照して更に説明される。

【図面の簡単な説明】

【００５１】

【図１】事前構成の間の無線ドッキング・システムを示す図。

【図２】ホストへの接続を確立する無線装置を示す図。

【図３】接続されている無線装置に指示する無線ホストを示す図。

【図４】更なる無線装置に直接接続される無線装置を示す図。

【発明を実施するための形態】

【００５２】

図は、単に概略であって、尺度通りに描かれているわけではない。図において、すでに説明された要素に対応する要素は、同じ参照符号を有する場合がある。

【００５３】

無線ドッキング・システムのための詳細な実施態様が以下で議論される。無線ドッキングは、携帯型装置(いわゆる無線ドッキーまたはWD)が無線周辺機器のグループに無線で接続することを可能にすることに関し、携帯型装置上のアプリケーションは、これらのアプリケーションの動作/インストラクションの経験及び生産性を改善するために、これらの周辺機器を使用することができる。周辺機器のグループ化、周辺機器のグループの発見及び周辺機器のグループへの接続の管理は、いわゆる無線ドッキング・ホスト(WDH)によって実行される。

【００５４】

考えられる無線ドッキーは、携帯電話、ラップトップ・コンピュータ、タブレット、携帯型メディア・プレーヤー、カメラを含む(但しこれらに制限されない)。考えられるWDHは、専用の無線ドッキング・ステーション装置、表示装置、オーディオ装置、プリンタ、PCを含む(但しこれらに制限されない)。考えられる周辺機器は、無線マウス、キーボード、表示装置、オーディオ装置、ウェブカメラ、プリンタ、記憶機器、USBハブを含む(但しこれらに制限されない)。これらの周辺機器は、他の装置(例えばドッキー及びWDH)への無線ネットワークを通してそれらの機能を利用可能にするためのWi-Fiシリアル・バス及びWi-Fiディスプレイのような規格をサポートすると考えられる。有線の周辺機器は、ワイヤを介してそれらを中間装置に接続することによって、無線ネットワークに接続されることができ、中間装置は、本明細書において定義されるように、無線で接続可能である(例えばWi-Fiシリアル・バスをサポートするUSBハブ装置)。周辺機器及びドッキーは、それ自身がWDHであることができる。

【００５５】

図1は、事前構成の間の無線ドッキング・システムを示す。無線ドッキング・システムは、無線ドッキング・ホスト装置H 100及びいくつかの無線周辺機器P1...Pn 110, 120, 1

30，140を有する。装置は、すべてWi-Fi無線トランシーバ101，111を備えており、Wi-Fi Direct P2Pグループに参加することをサポートする。いくつかの周辺装置は、P2Pクライアントまたはレガシー・クライアントとして動作することのみをサポートするように制限される場合がある。

【００５６】

図1は、無線ドッキングのための1セットの周辺機器を予め設定する初期状況を説明する。周辺装置は、Wi-Fi Direct接続150 SC1 ... SCnを通して、P2Pクライアントとして動作する周辺装置P1 ...Pn及びHによって形成されるP2Pグループのグループ・オーナー(P2P GO)として動作するホスト装置H100に接続される無線装置のグループ190を形成する。それに対して、無線装置は、P2Pクライアントの機能を有するとして示されるそれぞれの通信プロセッサ112を有する。実際には、そのような無線装置および/またはホスト装置の通信プロセッサは、それ自体知られており、専用の集積回路、プログラム可能な回路および/またはマイクロコントローラもしくは専用のプロセッサにおいて実行されるファームウェアとして実装されることができる。通信プロセッサは、以下で説明されるような通信プロセスを実行するように用意される。

【００５７】

Wi-Fi Direct 接続SC1 ... SCnを設定することは、例えばWi-Fi Simple Configuration (WSC)を用いたペアリング・ステップを必要とする。そして、ペアリング・ステップの間、Wi-Fi保護アクセス(WPA/WPA2)に基づくセキュアな接続を確立するために共通秘密S1がHによって提供される。秘密S1は、パスフレーズ(Wi-Fi ペアワイズ・マスター・キー(PMK)またはWi-Fi 事前共有キー(PSK))であることができ、Wi-Fi保護アクセス(WPA/WPA2)を設定するために４ウェイ・ハンドシェイクにおいて用いられる。

【００５８】

秘密S1を配信するための多くの可能性が存在し、例えば、秘密S1は、Wi-Fi Simple Configurationを用いて配信されることができ、あるいは、秘密S1は、全ての関連する装置中に予め設定されることができる。無線ドッキング・ホスト装置Hは、周辺機器に関する情報を記憶し、接続の経過を記録し、秘密を確立し、他の装置に指示するための、(無線ドッキング管理と呼ばれる)ホスト通信プロセッサ102を有し、どの周辺機器が無線ドッキング環境をともに形成するかを設定する。

【００５９】

図2は、ホストへの接続を確立する無線装置を示す。無線装置200はドッキーDと呼ばれ、上述の図1と同様の無線ドッキング・システムにおいて示される。無線装置は、Wi-Fi無線トランシーバ201、及び、通信プロセスを制御するための通信プロセッサPROC 202を有する。

【００６０】

システムにおいて、無線ドッキーDは、１セットの周辺機器とドッキングするために、無線ドッキング・ホストH 210とのWi-Fi Direct接続C 250を確立する。この特定の実施態様は、ドッキーが無線ドッキング・ホストHへの初期ドッキング接続(いわゆるパイロット接続)を設定するためのソリューションのみを示し、装置P1...Pnのいずれかへの接続は示さない。同様に、ドッキーは、更なる無線装置P1..Pnのいずれか１つが初期接続を設定するためのホスト機能を実行するように用意される場合には、そのような無線装置への初期接続を設定することができる。したがって、ホスト機能は、１つの装置によって実行されることができるか、あるいは、異なる装置の間で分配されることができる。

【００６１】

接続Cを設定するためのDとHとの間のペアリング・ステップの間、Hは、安全性の理由のために、Wi-Fi保護アクセス(WPA/WPA2)に基づくセキュアな接続を確立するために、S1と等しくない秘密S2がHによって提供されることを確実にする。接続ライン240によって示される秘密データS1に基づく接続SC1 ... SCnと同様に、秘密S2は、パスフレーズ(Wi-Fi ペアワイズ・マスター・キー(PMK)またはWi-Fi 事前共有キー(PSK))であることができ、Wi-Fi保護アクセス(WPA/WPA2)を設定するために４ウェイ・ハンドシェイクにおいて用いられ

る。秘密S2を配信するための多くの可能性が存在し、例えば、秘密S2は、Wi-Fi Simple Configurationを用いて配信されることができ、あるいは、秘密S2は、全ての関連する装置中に予め設定されることができる。この実施態様において、DはHのP2P GOに接続し、それによって、Dは自動的にP2Pクライアントになる。別の態様では、D及びHは、Hと周辺機器との間で確立されるP2Pグループから独立した新たなP2Pグループを形成し、それによって、DまたはHのいずれかは、P2P GOになることができる。

【００６２】

図3は、接続されている無線装置に指示する無線ホストを示す。無線ホストH 310は、上記の図1及び図2と同様の無線ドッキング・システムにおいて示される。

【００６３】

図は、ドッキーD200及び無線ドッキング・ホストH310から指示を受信する周辺機器P1...Pn 110,120を説明する。図は、Hが、指示I1...In 320を通して１つ以上の周辺機器に、さらに指示DI 330を通してドッキーに、周辺機器とDとの間の自動化されたペアリング・ステップの間に秘密S3を用いることについて指示することを示す。これらの指示及びメッセージは、MACフレームにおけるバイナリ符号化された指示からHTTP上のXML符号化された指示に及ぶ多くの異なる通信プロトコルを用いる任意のフォーマットを採ることができる。

【００６４】

秘密データS3に加えて、指示は、それを受信した後に装置が実行する必要がある動作（例えば、Hとの接続の切断やDとの接続の設定）に関する情報を含むことができる。周辺機器は、DがそのWi-Fi Direct能力を広告するために用いるサービスセット識別子SSIDに関する情報を提供されることを必要とする場合があり、Dは、接続を確立しようとする周辺機器の固有の識別子のような情報を提供されることを必要とする場合がある。１つ以上の周辺装置PiはHに接続されたままの場合がある。これらの装置は、Hに接続されたままでいるようにとの指示、またはHから切断するようにとの指示を受信することができる。図3において、装置P3...Pn-1が、Hに接続されたままでいるようにとの指示を受信すると仮定する。

【００６５】

チャネルCを使用して、秘密データS2から導き出されるキーによって保護されて、秘密データS3もドッキーDに送られる。これは、D及び１つ以上の周辺機器が、４ウェイ・ハンドシェイクを用いて、WPA/WPA2で保護された接続を直接設定することができること、並びに、PINコードを入力するという考え得るユーザ・インタラクションを伴う、Wi-Fi Simple Configuration手順の実行は必要とされないことを意味する。Wi-Fi Simple Configuration手順を実行する必要がないことは、ドッキング手順をスピードアップする。

【００６６】

図4は、更なる無線装置に直接接続される無線装置を示す。無線装置D 400は、上記の図1、2及び3と同様の無線ドッキング・システムにおいて示される。図は、ドッキーD 400、及び、直接接続されている、そしてオプションとして破線430で示されるように無線ドッキング・ホストH100から切断されている、周辺機器P1...Pnのサブセット(例えば3つの周辺機器110,120,140)を図示する。図では、１つの周辺機器130は、ドッキーDに接続されず、無線ドッキング・ホスト100にのみ接続されたままである。

【００６７】

図は、装置P1、P2及びPnが、420により示される秘密データS3(パスフレーズS3)を用いて、ドッキー装置Dとの直接接続SP1、SP2及びSPnを設定した状況を示す。Dは、SD1、SD2及びSDnのための(図においてP2P GOユニット403によって示される)Wi-Fi Directグループ・オーナーとして動作する。Hとの接続SC1、SC2及びSCnは、解除されてもよいし、有効のままでもよい。図4中の点線はこれを反映する。ドッキングは、役割を変更して無線周辺機器のサブセットのためのP2P GOになるドッキーDを含む。WPA/WPA2の４ウェイ・ハンドシェイクの間、S3は、リンク・キー(ペアワイズ一時キー)を導き出すための共通秘密(Wi-Fi ペアワイズ・マスター・キー(PMK)またはWi-Fi事前共有キー(PSK))として用いられる

ことができる。別の態様では、S3はWi-Fi保護設定（Protected Setup）ペアリング手順において用いられ、ユーザ入力（例えばPINコード）の代わりに、PINはS3から導き出される。

【００６８】

実際には、上記の無線ドッキング・システムは、待ち時間を低減するために、無線ドッキーDを表示装置または(USB)マウス/キーボードに直接接続するために適用されることができる。装置は、事前に決められた構成セットを用いるように指示されることができる。切断された装置は、スリープに入ることができる。オプションとして、無線ホストは、それらの装置に、それらを発見して再びそれらと接続することを可能にするために、特定の規則的なインターバルでウェイク・アップするように指示することができる。

【００６９】

一例のシステムにおいて、無線周辺装置P(例えばWi-Fiディスプレイ)は、パスフレーズS1に基づくリンク・キー(ペアワイズ一時キー)に基づいてセキュアチャネルCを介して無線ホストHに最初に接続されることができる。ホストはグループ・オーナー(GO)として動作し、Pはクライアントとして動作する。H及びPは両方ともWi-Fi Direct継続P2Pグループ化をサポートする。それに対して、Pは、そのメモリ中にパスフレーズS1を記憶する。ドッキーDは、パスフレーズS2に基づくリンク・キー(ペアワイズ一時キー)によるセキュアチャネルD上でWi-Fi Directを介して、最初にホストHと接続する。ドッキング構成プロトコルを介して、Hは、Wi-Fi上でのペイロード接続が受諾される必要があることをドッキーDに指示する。周辺機器Pとの直接接続は、周辺機器Pと合意されるリンク・キー(ペアワイズ一時キー)Mを生成するためにパスフレーズS3を用いて、Dにおけるグループ・オーナー・ユニットを介して遂行される。Hは、Dと合意されるリンク・キー(ペアワイズ一時キー)Mを用いて周辺機器DのGOに接続する必要があることをPに指示する。以下で、Pは、Hとの接続を切断することができ、リンク・キー(ペアワイズ一時キー)MによりDとのリンクを設定する。PとDとの間の接続が切断される場合(例えばDが切り離される場合)、Pは元のパスフレーズS1を用いてHに再接続することができる。

【００７０】

実際的な実施の形態において、上述の改善された無線ドッキング・システムは、以下のように実施されることができる。一例の無線ドッキング・システムにおいて、１つの無線ホストWDHが存在し、それを通して、無線装置WDはドッキングすることができる。WDHは、有線や無線のインタフェースを通して周辺機器PFに接続され、内蔵型PFを有することもできる。いくつかの無線PFは、それらが、ドッキングされたWDに直接接続するように指示されることができ、または無線ホスト機能を実行する能力を持つように、追加の組込み機能を有することをさらに仮定する。

【００７１】

以下の利点が、拡張無線ドッキング・システムによって達成される。PFは、(Wi-Fi Simple Configuration WSCプロトコルを実行するいかなる必要もなく)ユーザが操作しなくても、WDに迅速に接続されることができる。一度ドッキングを許されただけのWDは、切り離された後では、もはや、ドッキングされていたPF又はWDHに再度自動的に接続することは許されない。WDとそれがドッキングするWDHとの間のWi-Fi通信は、プライバシー及び整合性のために保護される。さらに、以前そのWDHとドッキングしていた可能性がある他のWDは、この通信を解読することができず、または、検出されずにそれを改竄することができない。WDとそれがドッキングの間に直接接続されるPFとの間のWi-Fi通信は、プライバシー及び整合性のために保護される。さらに、これらのPFと以前接続された可能性がある他のWDは、この通信を解読することができず、または検出されずにそれを改竄することができない。WDHとWi-Fi接続されたPFとの間の通信は、プライバシー及び整合性のために保護される。さらに、このWDHにドッキングするWDは、WDHからのいくつかのこの通信及びこのWDHにドッキングするWDから生じるいくつかのこの通信を受信するが、WDは、この通信を解読することができず、または検出されずにそれを改竄することができない。何度もドッキングすることを許可されるWDは、それが初めてドッキングするときに、一度のみWSCを

実行しなければならず、それが再びドッキングするときには、WSCを用いることなくドッキングすることができる。WDが自動的に常にドッキングさせることができるように、WD及びWDHは両方とも予め設定されることができる。

【００７２】

一例の拡張無線ドッキング・システムにおいて、以下のフェーズが定められる：制御されたまたは制御されていないセットアップ(または構成)フェーズ、ドッキング解除（undocked）・モード、ドッキング・フェーズ及びドッキング解除・フェーズ。

【００７３】

セットアップ・フェーズにおいて、WDHは、SSIDとしてSSID1及びパスフレーズとしてPP1を有するP2PグループG1のためのP2P GOとして、それ自体を設定する。WDHは、G1に参加するためのPFのみを受諾する。複数のPFは、PP1を得るためにPBCまたはWSC-PINを用いてG1に参加する。PFは、SSID1及びPP1のために予め設定されることができる。

【００７４】

ドッキング解除モードにおいて、WDHは、SSIDとしてSSID2を有するP2PグループG2のためのP2P GOとしてそれ自体を設定するが、依然としてG2のためのパスフレーズを決定しない。WDHは、G2のためのビーコン・フレームを送ることができる。WDHは、プローブ・リクエスト・フレームに応答する。WDHは、関連する情報要素（Information Element）において、それが、そのPF、そのWDEなどのWDHであるという情報を与える。WDHは、G2に参加するためのWDのみを受諾する。

【００７５】

ドッキング・フェーズにおいて、G2を発見したWDは、G2に参加することを要求する。これは、ドッキング動作をトリガーする。WDがドッキングすることを許可されない場合、要求されたドッキング動作は拒否される。WDが以前にドッキングしており、そのWDが再びドッキングすることを許可された場合、WDHは、G2のためのパスフレーズPP2として、それがそのWDと以前に用いたパスフレーズを設定する。全ての他の場合（したがって、WDが以前ドッキングしたことが無い場合、又は、以前ドッキングしたことはあるが、一度のみドッキングすることを許可されていた場合）、WDHは、G2のためのパスフレーズとして、新たなランダムなPP2を生成する。WDHは、P2PグループG1を用いて(したがってPP1から導き出されるキーによって暗号化され、したがって全てのWD及び全ての他の装置に対して秘密が保たれて)、全てのPFに、SSID2、PP2、WDアドレス及びWD IDを送る。WDがこのWDHのためのパスフレーズによって予め設定されている場合、または、前のドッキング・セッションからのパスフレーズを依然として所持している場合、それは、４ウェイ・ハンドシェイクにおいてそのパスフレーズを試みて用いることができる。そうでない場合、または以前のパスフレーズを用いることが失敗する場合、WDは、PP2を得るためにWDHとのP2PグループG2のためのWSCを実行する。WSCは、PBS、または、WDもしくはWDH PINを用いるWSC-PINを用いることができる。

【００７６】

G2に参加した後に、いかなるPFもWDHに直接接続されない場合、WD及びWDHは、WDHを通したPFへのペイロード接続を設定し、WDはドッキングされる。

【００７７】

１つ以上のPFがWDに直接接続される場合、WDはWDHとGOの役割を交換する。WDHは、WDへの直接Wi-Fi接続を設定することをサポートする全てのPFのアドレス/IDを送る。それは、何かの理由でWDHを通してペイロード接続が最良にルーティングされるPFのアドレスを除外することができる。我々は、これらを「直接」PFと呼ぶ。全ての他のPFは、「間接」PFと呼ばれる。通信手段としてP2PグループG1を用いて、WDHは、パスフレーズPP2を用いてP2PグループG2に参加するように直接PFに求める。事実上この例では、第２秘密データは、第３秘密データに等しい。直接PFが今ではPP2を知っているので、それらはG2に参加するためにWSCを実行する必要がなく、それは、例えばPINが事前設定されている場合であっても、相当な時間を節約する。これらのPFは、単に、それらが知っているパスフレーズ(PP2)を用いてWDとの４ウェイ・ハンドシェイクを実行する。WDは、関与する直接PFのアドレ

スを得ており、それによって、どのPFが接続を期待するのかを知る。G2を通したWD及びG1を通したPFの両方は、P2PグループG2参加が成功したか失敗したかをWDHに通知することができる。例えばPFとWDとの間の距離があまりに大きい場合、PFは、P2PグループG2に参加することに失敗する可能性がある。参加に失敗した直接PFは間接PFになり、WDHと接続されたままである。WDは、成功裏にG2に参加したPF(すなわち直接PF)のための直接ペイロード接続を設定する。これらのペイロード接続は、PP2から導き出されるキーを用いて保護される。WD及びWDHは、WDHを通した他のPF(すなわち間接PF)へのペイロード接続を設定し、WDはドッキングする。WDHが同時に複数のWDをサポートする場合、それはドッキングのための新たなWDを引き受けるために新たなSSIDを設定することができる。

【００７８】

ドッキング解除・フェーズにおいて、ドッキング解除は、制御されたまたは制御されていない態様で実行されることができる。制御されたドッキングは、それによって、WDが、それがドッキングを解くことを所望することをWDHに示す。制御されていないドッキング解除は、ドッキングを解くことを所望するというWDからの指示を受信せずに、WDが去ったか、または、連絡できなくなったことをWDHが何らかの形で検出することである。

【００７９】

制御されたドッキング解除の間、WDは、ドッキング解除を所望するときに、ドッキング解除を所望する通信手段としてのP2PグループG2を用いてWDHにメッセージを送る。WDHは、このメッセージの成功した受信を肯定応答する。そのメッセージの伝達が成功した後、WDは、G2において、理由コード3を有する認証解除フレームをWDH及びPFに送ることによって、P2PグループG2セッションを終える。認証解除フレームの受信に応じて、PFは、ペイロード接続を取り壊す。通信手段としてP2PグループG1を用いて、WDHは、用いられたPP2を削除するように直接PFに指示する。別の態様では、WDが再びドッキングすることを許可されない場合にのみ、これを実行することができる。この場合には、PFは、再びドッキングすることを許可されるWDでの後の利用のためにパスフレーズ及びWD IDの組み合わせを記憶しなければならない。これは、ドッキング動作の間の相当な時間を節約することができる。WDHは、どのPFを通してどのパスフレーズを受信したのかについて記録しなければならない。WDHは、間接PFにペイロード接続を取り壊すように指示する。WDHは、再びP2PグループG2のGO役割を引き受けて、パスフレーズを未決定に設定する。WDHは、再び、ドッキング解除状態を広告することができる。

【００８０】

制御されていないドッキング解除の間、WDHは、ドッキングを解くことを所望するというWDからの指示を受信せずに、WDが去ったか、または、連絡できなくなったことをWDHが何らかの形で決定する。WDHは、(直接または間接)ペイロード接続を取り壊すように、全てのPFに通知する。通信手段としてP2PグループG1を用いて、WDHは、用いられたPP2を削除するように直接PFに指示する。別の態様では、WDが再びドッキングすることを許可されない場合にのみ、これを実行することができる。この場合には、PFは、再びドッキングすることを許可されるWDでの後の利用のためにパスフレーズ及びWD IDの組み合わせを記憶しなければならない。これは、ドッキング動作の間の相当な時間を節約することができる。WDHは、どのPFを通してどのパスフレーズを受信したのかについて記録しなければならない。WDHは、再びP2PグループG2のGO役割を引き受けて、パスフレーズを未決定に設定する。WDHは、再び、ドッキング解除状態を広告することができる。

【００８１】

本発明が主に無線ドッキングを用いる実施の形態によって説明されたが、本発明は、接続されていない無線装置が装置のグループに接続する必要がある任意の無線システムのためにも適している。本発明は、Wi-Fiドッキング対応装置、Wi-Fiシリアル・バス装置、Wi-Fiディスプレイ装置、及び、携帯型オーディオ装置、携帯電話、ラップトップ・コンピュータ、タブレットから、Wi-Fiマウス、キーボード、表示装置、プリンタ、カメラに及ぶ、Wi-Fi Directをサポートする任意の他の装置に関する。

【００８２】

本発明は、プログラム可能なコンポーネントを用いて、ハードウェアおよび/またはソフトウェア中に実施されることができることに留意する必要がある。本発明を実施するための方法は、図1を参照して記述されるシステムに対して定められる機能に対応するステップを有する。

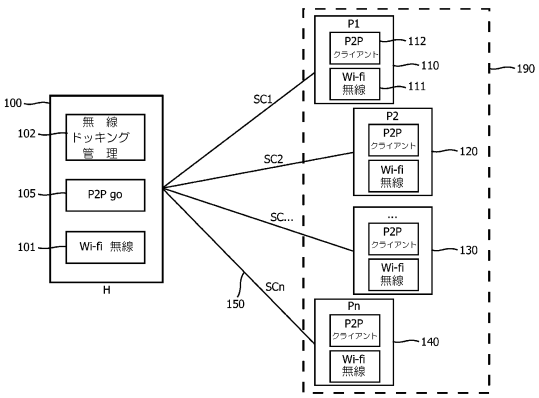
【００８３】

明確性のための前記説明が異なる機能ユニット及びプロセッサを参照して本発明の実施の形態を記述したことはいうまでもない。しかしながら、異なる機能ユニットまたはプロセッサ間での機能の任意の適切な分配が、本発明から逸脱せずに用いられることができることは明らかである。例えば、別々のユニット、プロセッサ又はコントローラによって実行されると説明された機能は、同じプロセッサ又はコントローラによって実行されることができる。したがって、特定の機能ユニットに対する参照は、単に説明される機能を提供するための適切な手段に対する参照として見なされるべきであり、厳密な論理的又は物理的構造又は機構を示すわけではない。本発明は、ハードウェア、ソフトウェア、ファームウェアまたはこれらの任意の組み合わせを含む任意の適切な形態で実施されることができる。

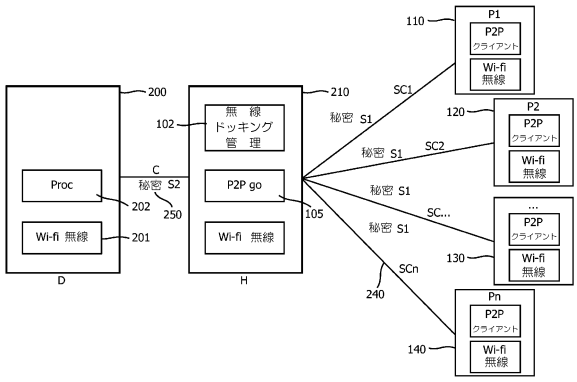
【００８４】

なお、本明細書において、「有する」「含む」等の用語は、挙げられたもの以外の他の要素又はステップの存在を除外せず、単数で表現された要素は、そのような要素が複数存在することを除外せず、如何なる参照符号も請求の範囲を限定せず、本発明は、ハードウェアおよびソフトウェア両方の手段によって実施されることができ、いくつかの「手段」又は「ユニット」は、ハードウェアまたはソフトウェアの同じアイテムによって表される場合があり、プロセッサは、おそらくハードウェア要素と協働して、１つ以上のユニットの機能を実現することができることに留意する必要がある。さらに、本発明は実施の形態に制限されず、本発明は、上記のまたは相互に異なる従属請求項中に列挙されるいずれ新規な特徴または特徴の組み合わせにもある。

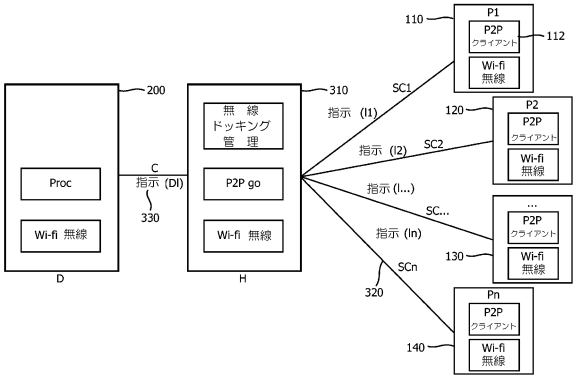
【図１】



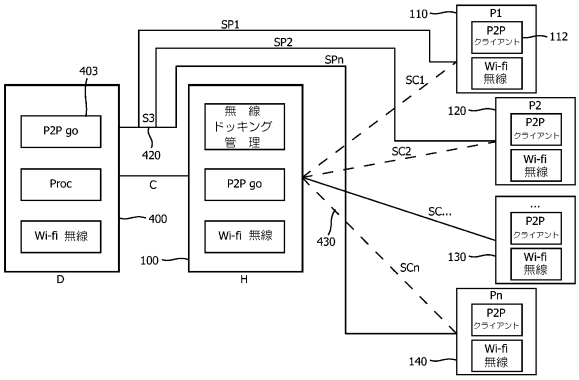
【図２】



【図３】


200
Proc
Wi-fi 無線
D
C
指示 (DI)
330
無 線
ドッキング
管 理
P2P go
Wi-fi 無線
H
310
指示 (I1)
SC1
指示 (I2)
SC2
指示 (I...)
SC...
指示 (In)
SCn
320
110
P1
P2P
クライアント
Wi-fi
無線
112
120
P2
130
...
140
Pn

【図４】


403
P2P go
Proc
Wi-fi 無線
D
S3
420
C
400
100
無 線
ドッキング
管 理
H
SP1
SP2
SPn
SC1
SC2
SC...
SCn
430
110
P1
P2P
クライアント
Wi-fi
無線
112
120
P2
130
...
140
Pn

フロントページの続き

(72)発明者　デース　ワルテル
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５
(72)発明者　ベルンセン　ヨハネス　アルノルドス　コルネリス
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５

審査官　三浦　みちる

(56)参考文献　特表２０１２－５１２６１２（ＪＰ，Ａ）
特開２００５－２０３８４６（ＪＰ，Ａ）
特開２０１２－０５００９６（ＪＰ，Ａ）
国際公開第２００９／０２７７７０（WO，Ａ１）
特開２０１１－１７６５８２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　　７／２４－　７／２６
Ｈ０４Ｗ　　４／００－９９／００
Ｈ０４Ｌ　　９／３２