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

特許第6328123号
(P6328123)

(45)発行日　平成30年5月23日(2018.5.23)　(24)登録日　平成30年4月27日(2018.4.27)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 673C |
| H04M 11/00 | (2006.01) | H04M | 11/00 | 303 |
| G06F 21/44 | (2013.01) | G06F | 21/44 | |
| H04W 12/02 | (2009.01) | H04W | 12/02 | |

請求項の数 19　(全 14 頁)

| | |
|---|---|
| (21)出願番号 | 特願2015-536059 (P2015-536059) |
| (86)(22)出願日 | 平成25年9月27日 (2013.9.27) |
| (65)公表番号 | 特表2016-504778 (P2016-504778A) |
| (43)公表日 | 平成28年2月12日 (2016.2.12) |
| (86)国際出願番号 | PCT/EP2013/070285 |
| (87)国際公開番号 | WO2014/056744 |
| (87)国際公開日 | 平成26年4月17日 (2014.4.17) |
| 審査請求日 | 平成28年9月16日 (2016.9.16) |
| (31)優先権主張番号 | 12188252.6 |
| (32)優先日 | 平成24年10月11日 (2012.10.11) |
| (33)優先権主張国 | 欧州特許庁 (EP) |
| (31)優先権主張番号 | 1218296.0 |
| (32)優先日 | 平成24年10月11日 (2012.10.11) |
| (33)優先権主張国 | 英国 (GB) |

(73)特許権者　513183153
ノルディック　セミコンダクタ　アーエスアー
Ｎｏｒｄｉｃ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒ　ＡＳＡ
ノルウェー王国、エヌ－７００４　トロンハイム、オットー　ニールセンス　ヴェーグ　１２
(74)代理人　110001807
特許業務法人磯野国際特許商標事務所
(72)発明者　エンゲリエン－ロペス、ダヴィッド　アレクサンドル
ノルウェー王国、７５６３　マルヴィック、スミカレット　６４

最終頁に続く

(54)【発明の名称】アドレス可能な無線装置

(57)【特許請求の範囲】

【請求項１】

連続した整数値として１ずつ増分する計数器を備えるアドレス可能な無線装置であって、

前記アドレス可能な無線装置は、（ｉ）前記計数器の現在の値と（ｉｉ）前記現在の値と前記無線装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを有し、

前記アドレス可能な無線装置は、前記アドレスを含む無線メッセージを送信するか、または、前記アドレスを含む無線メッセージを受信して応答するように構成される

ことを特徴とする、アドレス可能な無線装置。

【請求項２】

前記計数器の前記値は長さが２４ビットであり、前記ハッシュは長さが２４ビットである

ことを特徴とする、請求項１に記載のアドレス可能な無線装置。

【請求項３】

アドレスを生成する手段を備えている

ことを特徴とする、請求項１または請求項２に記載のアドレス可能な無線装置。

【請求項４】

前記ハッシュは、前記計数器の前記値を、前記身元解読キーを暗号化キーとして使用した高度暗号化標準（ＡＥＳ）によって暗号化した出力の関数である

ことを特徴とする、請求項１乃至請求項３のいずれか一項に記載のアドレス可能な無線

装置。
【請求項５】
前記身元解読キーは、１２８ビットの数である
ことを特徴とする、請求項１乃至請求項４のいずれか一項に記載のアドレス可能な無線装置。
【請求項６】
前記アドレスは、（ｉ）計数器の前記値と（ｉｉ）前記ハッシュとを連結したものである
ことを特徴とする、請求項１乃至請求項５のいずれか一項に記載のアドレス可能な無線装置。
【請求項７】
計数器を増分することによって、そのアドレスを一定の間隔で変更するように構成される
ことを特徴とする、請求項１乃至請求項６のいずれか一項に記載のアドレス可能な無線装置。
【請求項８】
ほぼブルートゥース低エネルギー装置として動作するように構成される
ことを特徴とする、請求項１乃至請求項７のいずれか一項に記載のアドレス可能な無線装置。
【請求項９】
アドレス可能な無線装置用のアドレスを生成する方法であって、前記方法は、
連続した整数値として１ずつ増分するように構成される計数器の値を決定することと、
（ｉ）前記値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを計算することと、を含む
ことを特徴とする方法。
【請求項１０】
計数器を増分すること、をさらに含む
ことを特徴とする、請求項９に記載の方法。
【請求項１１】
アドレス可能な無線装置を動作させる方法であって、前記方法は、前記装置が無線で（ｉ）連続した整数値として１ずつ増分するように構成される計数器の値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを送信することを含む
ことを特徴とする方法。
【請求項１２】
アドレス可能な無線装置を動作させる方法であって、前記無線装置は（ｉ）連続した整数値として１ずつ増分するように構成される計数器の値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを有し、前記方法は、前記無線装置が前記アドレスを含む無線伝送を受信して処理することを含む
ことを特徴とする方法。
【請求項１３】
無線装置を動作させる方法であって、前記方法は、前記無線装置が無線伝送を受信して処理することを含み、前記無線伝送は、第二の、送信側無線装置のアドレスを含み、前記アドレスは、（ｉ）連続した整数値として１ずつ増分するように構成される計数器の値と（ｉｉ）前記値と前記送信側無線装置の身元解読キーの組み合わせであるハッシュとを含む
ことを特徴とする方法。
【請求項１４】
前記受信ハッシュが、前記受信値と、前記送信側無線装置と関係付けられた格納済身元解読キーとの組み合わせのハッシュであることを前記装置が判定することと、

前記受信値が所定の鮮度条件を満たしていることを前記装置が判定することと、をさらに含む
ことを特徴とする、請求項１３に記載の方法。
【請求項１５】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられた格納済ローカル計数値よりも大きいことを含む
ことを特徴とする、請求項１４に記載の方法。
【請求項１６】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられたローカル計数値よりも大きい鮮度閾値量以下であることを含む
ことを特徴とする、請求項１４または請求項１５に記載の方法。
【請求項１７】
（ｉ）連続した整数値として１ずつ増分するように構成される計数器の値と（ｉｉ）前記値と送信側装置の身元解読キーの組み合わせであるハッシュとを含む、前記送信側無線装置のアドレスを含む無線伝送を受信し、
前記受信ハッシュが、前記受信値と、前記送信側無線装置と関係付けられた格納済身元解読キーとの組み合わせのハッシュであることを判定し、
前記受信値が、所定の鮮度条件を満たしていることを判定する、
ように構成される
ことを特徴とする無線装置。
【請求項１８】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられた格納済ローカル計数値よりも大きいことを含む
ことを特徴とする、請求項１７に記載の無線装置。
【請求項１９】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられたローカル計数値よりも大きい鮮度閾値量以下であることを含む
ことを特徴とする、請求項１７または請求項１８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、アドレス可能な無線装置に関する。
【発明の概要】
【０００２】
マスタ装置が周辺装置またはスレーブ装置と通信する、多数の近距離無線通信プロトコルが知られている。通信の目的は、例えば、周辺装置を制御するため、および／または、周辺装置からデータを受信したり周辺装置にデータを送信したりするためである。そのようなプロトコルには、ブルートゥース、ブルートゥース低エネルギー、ＡＮＴおよびＺｉｇｂｅｅ（登録商標）が含まれる。このような無線装置は、通常は、アドレス可能な装置である、つまり、付随する装置アドレスを持ち、そのアドレス宛無線メッセージ（メッセージの一部として装置アドレスを含む無線メッセージなど）に応答する（アクションを実行することによって、返信メッセージを送信することによって、など）ように構成されている。この装置は、通常は、システム内の他の装置宛の無線メッセージの少なくともいくつかを無視する。
【０００３】
スレーブ装置としては、例えば、無線心拍数モニタが考えられ、マスタ装置として動作する、ユーザの携帯電話によって制御することができる。携帯電話は、当該モニタから心拍数情報を収集し、それをユーザに表示することができる。
【０００４】
このような無線装置は、通常は、付随する装置アドレスを有し、データの送信者および

／または所定の受信者を決定するために、送信されるデータパケットに含まれる。装置アドレスは、すべてのデータフレームに含まれていてもよいし、交信開始時のみ告知メッセージなどに含まれていてもよい（その後は、代わりとして、なんらかのセッション識別子またはチャネル識別子を用いてもよい）。

【０００５】

したがって、ある人が、その人に関係付けられていることが知られている一つまたは複数の装置アドレスを傾聴することで身元特定、および／または追跡される可能性があり、例えば、その人に属している心拍数モニタや携帯電話のアドレスが該当する。これは、プライバシーの問題につながる。

【０００６】

このような問題に対処する一つのアプローチは、ブルートゥース低エネルギー仕様（２０１０年６月３０日公開のブルートゥースコア仕様４．０など）に例示されている。これによれば、装置は、静的な公開アドレスの代わりに「解読可能な非公開アドレス」を使用することができる。図１は、このような解読可能な非公開アドレス１の構造を示している。アドレスは、無作為に生成された２４ビットの乱数である「プランド（ｐｒａｎｄ）」で構成され、ハッシュ値である「ハッシュ（ｈａｓｈ）」と連結されている。「プランド」の最上位の２ビットは図示したように常に「０」と「１」に等しく、残りのビットは無作為であるが、すべて「０」に等しくてもすべて「１」に等しくてもいけない。「ハッシュ」の値は、高度暗号化標準（ＡＥＳ）暗号化アルゴリズムを使用して（ゼロ詰めして１２８ビットにした）「プランド」をデバイス固有な１２８ビットの「身元解読キー」（ＩＲＫ）で暗号化した結果の最下位２４ビットである。

【０００７】

当該装置は、「プランド」の新しい値を生成し、対応する新しい「ハッシュ」の値を計算することによって、その非公開アドレスを一定の間隔で変更することができる。傍観者にとっては、非公開アドレスは、デバイスが毎回アドレスを更新した後も一貫して身元特定または追跡されないように、（最上位の２ビットを除いて）無作為データであるように見える。しかし、最初の装置がすでにその身元解読キー（ＩＲＫ）を共有した他のデバイスであれば、引き続き非公開アドレスを用いて当該装置の身元を特定することができる。第二の装置は、解読可能な非公開アドレスを受信すると、順番に、自分が知っている各装置のＩＲＫを使用して、「ハッシュ」部分を復号化しようとする。特定のＩＲＫによる結果として、アドレスの「プランド」部分と一致する復号化された値が得られた場合、このアドレスはそのＩＲＫを正常に使用した装置に属しているに違いないので、これで、最初の装置の身元を特定したことになる。スレーブ装置（心拍数モニタなど）が解読可能な非公開アドレスを使用して自らを告知した場合、盗聴者は、アドレス変更の間隔よりも長くは当該スレーブ装置（およびそれを携行する人）を身元特定または追跡することができないはずである。同様に、マスタ装置（携帯電話など）がスレーブ装置をスキャンしたりスレーブ装置に接続したりするときに解読可能な非公開アドレスを使用する場合、盗聴者は、アドレス変更の間隔よりも長くは当該マスタ装置（およびそれを携行する人）を身元特定または追跡することができないはずである。

【０００８】

しかし、出願人は、第三者が積極的に既知の相手として（つまり、ホワイトリストの装置として）なりすました場合、そのようなアプローチは、まだプライバシー攻撃に対して脆弱であり得ることを認識するに至った。したがって、本発明は、より良いアプローチを提供することを目的とする。

【０００９】

本発明は、第一の態様から言うと、（ｉ）計数器から得られる値と（ｉｉ）前記値と当該装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを有する、アドレス可能な無線装置を提供する。

【００１０】

このようにすれば、装置は、本発明によって、計数器に基づくアドレスを使用し、計数

器を増分することによって新しい装置アドレスを生成することができることを、当業者は理解できるであろう。重要な点は、これによって、古いアドレスは、現在および将来のアドレスとは容易に区別することができることである。第二の相手装置は、第一の装置のアドレスを受信すると、当該アドレスの値が、第二の装置との以前の通信で第一の装置が使用したアドレスの場合よりも高い計数器の値から得られたことを確認することによって、当該アドレスは新しいものであることを確認することができる。このような（または類似の）確認を行なうことで、攻撃者が、第二の装置から身元特定可能な応答を誘発することを目的として、無線通信の事前盗聴を通じて取得した、第一の装置の装置アドレスを含むメッセージを送信することによって、既知である、第一の装置になりすますという、第二の装置に対するプライバシー攻撃の機会を減少させることができる。第二の装置は、攻撃者によって提示された装置アドレスが古いアドレスであると判定した場合、応答しないようにすることで、身元特定したり追跡したりしようとする試みを阻止することができる。

【００１１】

本発明は、さまざまな態様から見ることができる。

【００１２】

本発明は、第二の態様で言えば、アドレス可能な無線装置用のアドレスを生成する方法を提供するものであって、前記方法は、

計数器から値を得ることと、

（ｉ）前記値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを計算することと、を含む。

【００１３】

前記方法は、さらに、計数器を増分すること、を含むことが好ましい。

【００１４】

本発明は、第三の態様で言えば、アドレス可能な無線装置を動作させる方法を提供するものであって、前記方法は、前記装置が無線で（ｉ）計数器から得られる値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを送信することを含む。前記アドレスは、告知メッセージに含まれていてもよい。

【００１５】

本発明は、第四の態様で言えば、アドレス可能な無線装置を動作させる方法を提供するものであって、前記無線装置は（ｉ）計数器から得られる値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを有し、前記方法は、前記無線装置が前記アドレスを含む無線伝送を受信して処理することを含む。

【００１６】

本発明は、第五の観点で言えば、無線通信装置を動作させる方法を提供するものであって、前記方法は、第二の、送信側無線装置のアドレスを含む無線伝送を前記装置が受信して処理することを含み、前記アドレスは、（ｉ）計数器から得られる値と（ｉｉ）前記値と前記送信側装置の身元解読キーの組み合わせであるハッシュとを含む。前記第一の無線装置は、アドレス可能であってもよい、つまり、それは、第一の装置アドレスに関係付けられていて、その装置アドレスに宛てた（例えば、前記アドレスを含む）無線メッセージに応答するように構成されてもよい。前記無線伝送は、必須ではないものの（例えば、前記伝送は、特定アドレス宛ではなく宛先の無い告知イベントであってもよい）、第一の、受信側無線装置のアドレスも含んでいてもよい。

【００１７】

いくつかの実施形態では、装置アドレスは、（新規のアドレス形式を使用すること以外は）ほぼブルートゥース低エネルギー仕様で定義されているように実質的に、告知用プロトコルデータユニット（ＰＤＵ）、走査用ＰＤＵまたは開始用ＰＤＵに含まれることもある。

【００１８】

無線装置は、ハードウェアロジックおよび／またはソフトウェアを実行するマイクロコントローラのような、アドレスを計算または生成する手段を備えていることが好ましい。当

該装置は、前出の値を計数器から得るように構成されていることが好ましい。当該計数器は当該装置から離れていてもよいが、当該装置が当該計数器を備えていることが好ましい。例えば、計数器は、装置の無線送信および／または受信手段または回路と共通の筐体内に配置してもよい。計数器は、計数値を維持し増分するように構成されたハードウェアおよび／またはソフトウェアを備えていてもよい。例えば、多くのフリップフロップを備えていてもよいし、マイクロコントローラ上で動作するファームウェアがメモリに格納する変数としてなどのように実現してもよい。計測器は、複数の無線伝送またはセッションにまたがって現在のカウント値を格納または維持するように構成されていることが好ましく、装置内の他の回路が電力供給されていなかったりスリープ状態であったりするときも含む。装置は、現在の計数値を不揮発性メモリに格納してもよいし、装置内の他の回路が電力供給されていなかったりスリープ状態であったりしても計数器メモリへの電力を維持するように構成されていてもよい。計数器のリセット機構を設けることもある。

【００１９】

計数器は、任意の適切な方法で計数すればよい。好ましい実施形態では、連続した整数値で増分する計数器である。計数器から得られる値は、単純に、計数器の現在値であってもよい。しかし、計数器出力の倍数のような、計数器の値のなんらかの関数であってもよい。好ましい一連の実施形態では、この値は、最上位の次のビット位置が「１」で最上位のビット位置が「０」である二つの付加ビットを併せ持つ計数器出力である。この値の合計の長さは、２４ビットであればよい。このような形式にすると、既存のブルートゥース低エネルギー装置との互換性を提供することができる。

【００２０】

装置は、計数器を増分するように構成されることが好ましい。定期的に、または、特定の条件が満たされたときこれを行なうように構成すればよい。これについては、以下でより詳細に説明する。計数器は、装置が作動したときに開始値（ゼロなど）に初期化されることが好ましい。装置は、リセット条件が成立したときに計数器を開始値にリセットするように構成してもよい。

【００２１】

計数器は、通常の使用においては、装置の予想寿命の期間中には桁あふれしない十分な容量のものであることが好ましい。例えば、少なくとも$2^{10}$個の一意的な値、好ましくは少なくとも$2^{20}$個の一意的な値を有する計数器であればよい。好ましい一連の実施形態では、２２ビット計数器である。

【００２２】

ハッシュは、任意の適切な形をとることができる。装置は、ハッシュアルゴリズムを値と身元解読キーとに適用するように構成されることが好ましい。ハッシュアルゴリズムは、値と身元解読キーに適用されて、その出力からキーを決定することが実行不可能または達成不可能であるような方法で出力を生成することが好ましい。ハッシュは、与えられた出力から、関数によってその出力が生成される値とキーを決定することは実行不可能または達成不可能であることが好ましい。ハッシュは、高度暗号化標準（ＡＥＳ）アルゴリズムを使用することが好ましく、その際に身元解読キーを暗号化キー（１２８ビットのキーが好ましい）として使用することが好ましく、計数器から得られる値を（必要に応じてゼロビットで桁詰めするなどして適切な長さにし）暗号化することが好ましい。ハッシュは、暗号化操作した結果を切り捨てた出力であってもよい。ハッシュは、出力の最下位２４ビットから成るような、ＡＥＳ演算の出力の関数であることが好ましい。こうすれば、合計アドレスのサイズを小さくし、より効率的な伝送をもたらすことができる。既存のブルートゥース低エネルギー装置との互換性を提供することもできる。ハッシュは、ブルートゥースコア仕様（バージョン４．０など）の「ランダムアドレスハッシュ関数ａｈ」として算出されることが好ましく、ここでrは、計数器から得られる値である。

【００２３】

身元解読キーは、１２８ビットの数であってもよい。装置に特有のものであることが好ましい。装置のメモリに格納してもよい。別の装置が当該キーを知ると、アドレスから第

一の装置の身元を判定することができることが好ましい。身元解読キーの本質と本発明を具体化した装置による使用は、ほぼブルートゥースコア仕様（バージョン４．０など）の中で身元解読キーについて説明されている内容のとおりである。

【００２４】

装置は、計数器から得られる値からアドレスを生成するように構成されることが好ましい。アドレスは、ハッシュと連結される値であることが好ましい。ハッシュの最下位の８ビットは、アドレスの最下位の８ビットになり、値の最上位の８ビットは、アドレスの最上位の８ビットになるものとする。装置は、メモリを備えて、アドレスをそのメモリに格納することができる。装置は複数のアドレスを有することもあるが、少なくともいくつかの実施形態において、装置は一つのアドレスだけを有する。

【００２５】

装置は、ほぼブルートゥース低エネルギー装置として、つまりブルートゥースコア仕様（バージョン４．０など）で定義されているとおりに動作するよう構成されていることが好ましい。

【００２６】

装置は、告知メッセージなどのように、自分のアドレスを含む無線メッセージを送信するように構成してもよい。このような装置は、ブルートゥースコア仕様（バージョン４．０など）で定義されているとおりに、ほぼブルートゥース低エネルギーのスレーブ役割にしたがって、スレーブ装置として動作するように構成することができる。アドレスは、任意の適切な方法で符号化することができる。デバイスは、計数器を増分することによって時々、好ましくは約１５分ごとなど一定の間隔で、そのアドレスを変更するように構成してもよい。

【００２７】

装置は、ブルートゥースコア仕様（バージョン４．０など）で定義されているとおりに、ほぼブルートゥース低エネルギーのマスタ役割にしたがって、マスタ装置として動作するように構成することができる。そのアドレスを含むスキャン用または接続用の無線メッセージを送信するように構成されてもよい。このような装置は、スレーブ装置との接続確立が完了した後に、計数器を増分することによってそのアドレスを変更するように構成することができる。

【００２８】

装置は、第二の装置から当該第二の装置のアドレスを含む無線メッセージを受信するように構成することができ、受信アドレスは、（ｉ）計数器から得られる値と（ｉｉ）前記値と前記第二の装置の身元解読キーの組み合わせであるハッシュとを含む。装置は、他の無線装置に関係付けられた、一つ以上の相手方の身元解読キーを格納してもよい。受信アドレスの値のハッシュを相手方身元解読キーの一つを使用して算出し、算出したハッシュが受信アドレスにあるハッシュと一致するかどうかを判定するように構成されていてもよい。各相手方の格納済身元解読キーを試み、一致するものが見つかれば、それによって第二の装置の身元を特定し、見つからなければ（装置が既知ではない場合）すべてのキーを試みる。第一の装置は、各相手方装置と関係付けられたローカル計数値、または身元解読キーを格納することが好ましい。第一の装置は、第二の装置の身元を特定した後、受信アドレスの値が所定の鮮度条件を満たしているか否かを判定するために、ローカル計数値を使用することが好ましい。この鮮度条件は、ローカル計数値よりも大きい受信値が計数器から得られることを含んでいてもよい。これにより、攻撃者が、装置によってすでに使用された補足アドレスを再生することによって既知の装置を模倣していないことを確認するために使用することができる。この条件は、ローカル計数値よりも大きい鮮度閾値量以下である受信値が計数器から得られることを含むこともできる。この鮮度閾値によれば、第二の装置が、第一の装置との通信が途切れた状態でもまだ鮮度条件を満たすことができる時間の上限を事実上設定することができる。第二の装置が、１５分ごとにそのアドレスを変更するスレーブ装置である場合、鮮度閾値は、約一年に相当する３５、０００ぐらいということになる。しかしながら、これよりはるかに小さくて１００または１、０００ぐら

いなどのこともあれば、それを上回って１００、０００以上ぐらいであることもある。このような鮮度閾値を適用することによって、攻撃者が、第一の装置との最後の通信後に第二の装置によって送信されたアドレスを捕捉し、そのようなアドレスを使用して第一の装置になりすます機会を制限することができる。鮮度条件が満たされない場合、装置は、無線伝送を拒否することが好ましい。それが満たされた場合、ローカル計数値は、受信アドレスの値が得られた計数に対応して更新されて、装置間の通信がさらに進められることが好ましい。

【００２９】

いくつかの実施形態では、第一の装置は、１５分ごとなど定期的にローカル計数値を増分することができ、こうすれば、マスタ装置によって格納されたローカル計数値が第二の装置であるスレーブ装置で使用される計数とほぼ同期が取れた状態を維持することができ、より小さい鮮度閾値を受容できるようにすれば、攻撃者が第二の装置になりすます機会をさらに制限することができる。

【００３０】

いくつかの実施形態では、計数値および／またはローカル計数値は、２２ビットなどの有限精度を使用して格納することができる。モジュロ演算の桁あふれとなる可能性がある。第一の値が第二の値よりも「大きい」ということは、第一の値が第二の値よりもモジュロの二分の一または別の適切な分数の分だけ先にある場合、第二の値よりも大きいと解釈できるなどといった文脈で、適切に定義することができる。

【００３１】

本発明は、第六の態様で言えば、無線装置を提供するものであって、前記無線装置は、

（ｉ）計数器から得られる値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含む、送信側無線装置のアドレスを含む無線伝送を受信し、

前記受信ハッシュが、前記受信値と、前記送信側無線装置と関係付けられた格納済身元解読キーとの組み合わせであることを判定し、

前記受信値が、所定の鮮度条件を満たしていることを判定する、

ように構成される。

【００３２】

このような無線装置は、それ自体が、（ｉ）計数器から得られる値と（ｉｉ）前記値と前記装置の身元解読キーの組み合わせであるハッシュとを含むアドレスを有してもよいが、必須ではない。鮮度条件に関する、上記の任意の特徴のいずれかを実装してもよい。

【００３３】

本発明は、さらなる態様で言えば、第一の無線装置と第二の無線装置を備えた通信システムを提供するものであって、前記第一の無線装置は、

（ｉ）計数器から得られる値と（ｉｉ）前記値と前記第一の無線装置の身元解読キーの組み合わせであるハッシュとを含む、前記第一の無線装置のアドレスを含む無線伝送を送信し、

第二の無線装置は、

前記無線伝送を受信し、

前記受信ハッシュが、前記受信値と、前記第一の無線装置と関係付けられた格納済身元解読キーとの組み合わせであることを判定し、

前記受信値が、所定の鮮度条件を満たしていることを判定する、

ように構成される。

【００３４】

前述の態様のいずれかに係る無線装置は、自らの身元解読キーを別の装置に送信するか、および／または、別の無線装置から身元解読キーを受信するように構成されることが好ましい。このようなキーの送信または交換は、ほぼブルートゥースコア仕様（バージョン４．０など）に記載されているとおりに行なわれることが好ましい。

【００３５】

前述の態様のいずれかに係る無線装置は、無線送信機および／または無線受信機を備え

ることが好ましい。本明細書に記載のステップを実行するための処理手段を備えていることが好ましい。このような処理手段は、ＣＰＵ、マイクロコントローラ、マイクロプロセッサ、ＡＳＩＣおよびＦＰＧＡのうち任意の一つ以上を備えることができる。本発明は、処理手段を備える無線装置上で実行されると、当該処理手段が本明細書に記載された方法のいずれかを実行する命令を含むソフトウェア（ファームウェアなど）にまで及ぶ。

【００３６】

一連の実施形態では、装置アドレスにある、計数器から得られる値は、計数器から得られる暗号化された値（暗号化された計数値など）であってもよいしそれを含むものであってもよい。身元解読キーのような装置固有キーで暗号化されてもよい。この値は、高度暗号化標準（ＡＥＳ）暗号化アルゴリズム（例えば、装置アドレスの１２８ビットを占有する）、または他のアルゴリズム（例えば、２４ビットの暗号化された値を出力する暗号化アルゴリズム）を用いて暗号化されてもよい。受信側無線装置は、対応する復号鍵を使用して、受信した暗号化された値を復号化すればよい。このような暗号化を使用する際に、アドレスにあるこの値の部分を、適切なキーを所有しない者にはランダムかつ予測不可能であるように見せることによって、攻撃者が装置を追跡する可能性をさらに減少させることができる。

【００３７】

他の実施形態では、計数器から得られる値が、計数器から得られる値のハッシュ（計数値の２４ビットのハッシュなど）であるか、またはそれを含むことによって、同様の効果を達成することができる。このハッシュは、身元解読キーのようなキーを使用して、例えば、先に記載したのと同じハッシュアルゴリズムを使用して計算されることが好ましい。受信側装置が、受信ハッシュから、計数器から得られる元の値を再構築することができるとは限らないので（ハッシュ関数は、通常は、一方向関数であるため）、受信側装置は、連続するローカル計数値に基づいて一連の正当なハッシュ値を生成し、受信ハッシュが一連の正当なハッシュ値の一つと一致することを確認するように構成してもよい。当該一連の値は、前述のようにして格納済ローカル計数値から始まり増分されるローカル計数値に基づいて、異なるハッシュ値となる鮮度閾値数を含んでいてもよい。

【００３８】

別の一連の実施形態では、計数器から得られる値は、線形フィードバックシフトレジスタ（ＬＦＳＲ）または他の擬似乱数発生器から得ることも可能で、連続するＬＦＳＲの各出力または擬似乱数の各出力は計数器増分に相当する。この場合も、受信側装置は、受信値を、送信側装置と関係付けられたローカル計数を元とし、同様の位置付けにある値の鮮度閾値数を含むこともある、ローカルに生成された一連のＬＦＳＲまたは擬似乱数値と比較するように構成することができる。

【００３９】

本明細書に記載の一態様または一実施形態の任意のまたは好ましい特徴は、適切である限り、他の態様または実施形態にも適用することができる。

【図面の簡単な説明】

【００４０】

本発明の特定の好ましい実施形態について、付随する図面を参照しながら、ほんの一例として説明することにする。

【図１】従来技術で知られている無線装置アドレスを図に表わしたものである。

【図２】本発明に係る無線装置アドレスを図に表わしたものである。

【図３】本発明を具現化した二台の無線装置と悪意のある装置の概略図である。

【図４】本発明を具現化したマスタ無線装置によって実行されるステップの流れ図である。

【図５】本発明を具現化したスレーブ無線通信装置によって実行されるステップの流れ図である。

【発明を実施するための形態】

【００４１】

図２は、本発明を具現化した無線装置のアドレスを示している。計数器の計数数値からなる２４ビットの計数部である「カウント」を有し、「１」と「０」のビットと連結されている。また、高度暗号化標準（ＡＥＳ）の暗号化アルゴリズムを使用して、（１２８ビットにゼロ詰めされた）「カウント」を（身元解読キーまたはＩＲＫと称される）デバイス固有の１２８ビットキーで暗号化した結果のうち最下位２４ビットである、「ハッシュ」という２４ビットのハッシュ部分も有している。

【００４２】

図３は、第一の無線装置３を示しており、ほぼブルートゥースコア仕様４．０で定義されているとおりに、マスタとなるブルートゥース低エネルギー装置である。これは、無線回路４と、マイクロコントローラ５と、さらに無線アンテナ６とを有している。また、スレーブとなるブルートゥース低エネルギー装置である第二の無線装置７も示してある。これも、無線回路８と、マイクロコントローラ９と、アンテナ１０と、を有している。第二の装置７は、本目的のために、第一の無線装置３の相手方となる（ペアを組む）ものとする。このように相手同士となる結果、第一および第二の無線装置３、７は、お互いの身元解読キー（ＩＲＫ）をそれぞれのマイクロコントローラ５、９がアクセス可能なようにすることになる。

【００４３】

最後に、第三の無線装置１１も示されているが、これは悪意のある攻撃者の制御下にあるものとする。攻撃者は、第一の無線装置３の所有者の動きを追跡する目的などのために、第一の無線装置３が第三の装置１１の近傍にあるときを判定したいと切望している。第一の装置が自らの静的な装置アドレスを含むメッセージを送信する場合、これは簡単である。ブルートゥースコア仕様４．０は、これを阻止するために解読可能非公開アドレス（ＲＰＡ）というメカニズムを提供している。しかし、攻撃者は、第二の無線装置７による、告知メッセージのような通信を盗聴することによって、つまり、メッセージに含まれる第二の装置７の装置アドレスを書きとめ、その後、このアドレスを含む自分自身の告知メッセージを送信し（つまり、第二の装置７を偽装し）第一の装置３からの応答を誘発するようにして、これを回避することができる。第一の装置３から、このような応答を受信した場合、このことを利用して、第一の装置３は第三の装置１１の近傍にあると判定することができる。

【００４４】

しかし、第一および第二の無線装置３、７に本発明を具現化させることによって、このような攻撃は、第一の装置３によって高い確率で検出することができる。その理由は、第二の無線装置７は、図２に示すようなアドレスを使用し、「カウント」の値を定期的に更新するからである。攻撃者は、第三の装置１１に第二の装置７から聴取したアドレスを再生させることができるだけであり、アドレスのハッシュ部分を計算するためのＩＲＫを知らないので、将来のアドレスを生成することはできない。第一の装置３は、第三の装置１１からの告知メッセージ内にある期限切れアドレスを受信したかどうかを識別し、応答しないことを選択することで、攻撃を阻止することができる。

【００４５】

図４は、本発明を具現化し、ほぼブルートゥースコア仕様４．０で定義されているとおりに、相手であるスレーブ装置については、マスタの役割で動作する無線装置によって行われるステップを示している。マスタ装置は、ペアを組む動作（図示せず）を通じてスレーブ装置のＩＲＫを知っており、スレーブ装置からの告知メッセージを問題無く受信し検証した後に、スレーブ装置に対するローカル変数である「リモート計数」をスレーブ装置の直近で解読したアドレスで維持・更新する。また、２２ビット変数である「ローカル計数」も格納し、それを使用して、図２に示すフォーマットを有する自分自身のマスタ装置アドレスを生成する。マスタ装置アドレスにある値「カウント」は、図２に示すように、「ローカル計数」の現在の値がビット「１」と「０」と連結されることによって得ることができる。これらの変数は、最初に作成されたときにゼロに初期化される。

【００４６】

マスタ装置が、本発明の実施形態に係るスレーブ装置の解読可能な非公開アドレスを（ＡｄｖＡフィールド内などに）含む、特定宛または不特定宛の告知メッセージを受信すると、まずスレーブ装置の身元を特定しようとする。その方法は、マスタ装置が知っているスレーブの各ＩＲＫを、上述したＡＥＳに基づくハッシュアルゴリズムを使用して、受信したスレーブ装置アドレスの「カウント」の値に適用し、受信アドレスにある「ハッシュ」の値と同一である出力を生成するものを見つけるまで、順番に行なう。何も見つからない場合、その告知は廃棄される。同一となるＩＲＫが見つかった場合、当該装置は、受信した「カウント」が有効基準を満たすかどうか確認する。満たさない場合、その告知は破棄される。「受信計数」は、「カウント」から最上位の２ビットを除去することによって抽出される。有効基準とは、「受信計数」が「リモート計数」よりも大きく、「受信計数」から「リモート計数」を差し引いたものが鮮度閾値である「非公開計数」よりも小さいことである。いくつかの実施形態では、「非公開計数」は、普通のスレーブ計数器の増分のほぼ一年に相当する３５、０００に等しく設定するものとする。もちろん、他の値を使用することもできる。演算は、常に正の値であるモジュロ$2^{22}$を用いて実行される。２２ビット計数器は、１５分ごとのスレーブ計数器の増分であればほぼ１２０年ごとに桁あふれすることになる。

【００４７】

マスタ装置は、確認して問題がなかった場合、なんらかの応答メッセージで使用するために、受信したスレーブアドレスを格納する（またはすでに保存した同内容を更新する）。「ローカル計数」の現在値を使用して、自分自身のアドレスも更新する。その後、「ローカル計数」の値を増分し、「リモート計数」を「受信計数」と等しくなるように設定する。また、接続を確立するなど、スレーブ装置に対して必要な応答を続行する。

【００４８】

２２ビット計数器が桁あふれに近い状態のとき（現実世界の実装で起こることは稀であるが）に起こりえる動作の例として、マスタ装置が、「受信計数」の値として１，０００を有する解読可能非公開アドレス（ＲＰＡ）を併せ持つ告知パケットを受信し、「非公開計数」を１０，０００に設定したと仮定する。マスタ装置の「リモート計数」は現在４，１９４，０００に設定されていると仮定する。すると、「受信計数」の値からモジュロ$2^{22}$（４，１９４，３０４）で「リモート計数」の値を差し引くと１，３０４となり、「非公開計数」よりも小さい。したがって、接続要求パケットが送信され、接続の確立が開始されることになる。次いで、「リモート計数」は「受信計数」の値に設定される。しかし、上記と異なり「非公開計数」が１，０００に設定されていた場合、「受信計数」の値からモジュロ４，１９４，３０４で「リモート計数」の値を差し引くと、「非公開計数」より大きくなり、接続要求パケットを送信してはいけないことになる。

【００４９】

無線装置で実行中のソフトウェアアプリケーションが「非公開計数」を低すぎる値に設定した場合、低い値であると、比較対象がそれを上回ると、計数値をリセットするために強制的に再接続が発生するので、使いやすさの点で問題となる可能性がある。しかし、「非公開計数」が高すぎる設定である場合、第二の装置は、かなりの時間にわたって（だまされて、既知である相手の装置を装った攻撃者に応答することによって）自分が追跡されていることを知らずにいることになるので、積極的なプライバシー攻撃に対する保護がおろそかになる。

【００５０】

図５は、本発明を具現化し、ほぼブルートゥースコア仕様４．０で定義されているとおりに、相手であるマスタ装置については、スレーブの役割で動作する無線装置によって行われるステップを示している。スレーブ装置は、ペアを組む動作（図示せず）を通じてマスタ装置のＩＲＫを知っており、マスタ装置からの接続メッセージを問題無く受信し検証した後に、マスタ装置に対するローカル変数である「リモート計数」を（ＩｎｉｔＡフィールドなどから取得して）直近で解読したマスタ装置のアドレスで更新・維持する。また、２２ビット変数である「ローカル計数」も格納し、それを使用して、図２に示すフォー

マットを有する自分自身のスレーブ装置アドレスを生成する。スレーブ装置アドレスにある値「カウント」は、図２に示すように、「ローカル計数」の現在の値がビット「１」と「０」と連結されることによって得ることができる。これらの変数は、最初に作成されたときにゼロに初期化される。

【００５１】

初期化した後、スレーブ装置は、「ローカル計数」の現在値を使用して自分自身のアドレスを設定する。また、「リモート計数」の現在値に基づいて、（ペアを組む動作からスレーブ装置が知っている）マスタ装置のＩＲＫを使用してマスタ装置のアドレスを生成し格納する。

【００５２】

スレーブ装置が接続要求に応答していないときであろうとも、「ローカル計数」を１５分ごとに増分する。もちろん、他の増分間隔であってもかまわない。

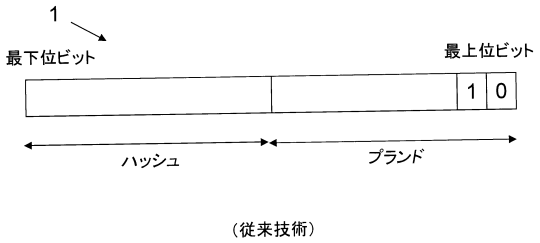
【００５３】

スレーブ装置が、本発明の実施形態に係るマスタ装置の解決可能非公開アドレスを含む接続メッセージを受信すると、まず、マスタ装置の身元を検証する。その方法は、マスタ装置のＩＲＫを、上述したＡＥＳに基づくハッシュアルゴリズムを使用して、受信したマスタ装置アドレスの「カウント」の値に適用し、出力が、受信アドレスにある「ハッシュ」の値と同一であることを確認する。一致しない場合、接続メッセージは廃棄される。一致する場合、スレーブ装置は、受信した「カウント」が有効基準を満たすかどうか確認する。満たさない場合、接続メッセージは破棄される。「受信計数」は、「カウント」から最上位の２ビットを除去することによって抽出される。有効基準とは、「受信計数」が「リモート計数」よりも大きく、「受信計数」から「リモート計数」を差し引いたものが鮮度閾値よりも小さいことである。いくつかの実施形態では、この鮮度閾値は、１，０００であって、許容範囲の使いやすさを維持しつつ攻撃者から適切に保護することができると期待されている。もちろん、他の値を使用することもできる。演算は、常に正の値であるモジュロ$2^{2^2}$を用いて実行される。

【００５４】

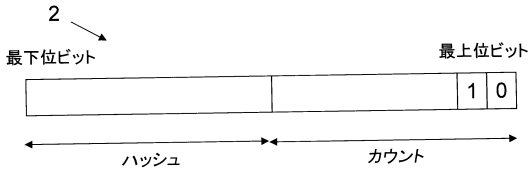
スレーブ装置は、確認して問題がなかった場合、「ローカル計数」の値を増分し、「リモート計数」を「受信計数」と等しくなるように設定する。新しい値を使用して、マスタ装置の格納済アドレスと自分自身のアドレスを更新する。また、自分との接続を確立するなど、マスタ装置に対して必要な応答を続行する。このようにして、マスタ装置３とスレーブ装置７の両方とも、攻撃者がそれらの身元を知って追跡する可能性を低減することができる。マスタ装置３は、最大限保護されるためには、相手となるすべてのスレーブ装置が、本発明に係る、計数器に基づくアドレスを使用することを要求するべきである。しかし、スレーブ装置によっては比較的まれにしかマスタ装置と通信しなかったり、攻撃者の範囲外であったりして、上記に当てはまらない場合でも、ある程度の保護を得ることができる。

【図１】

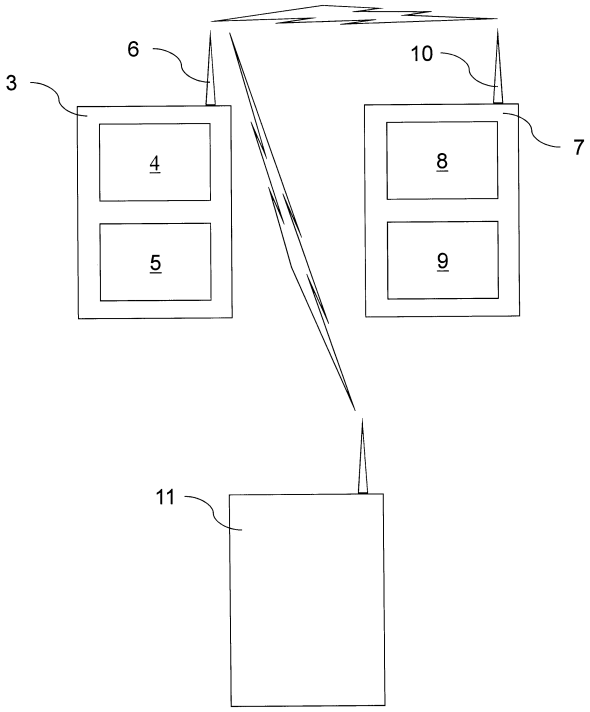



（従来技術）

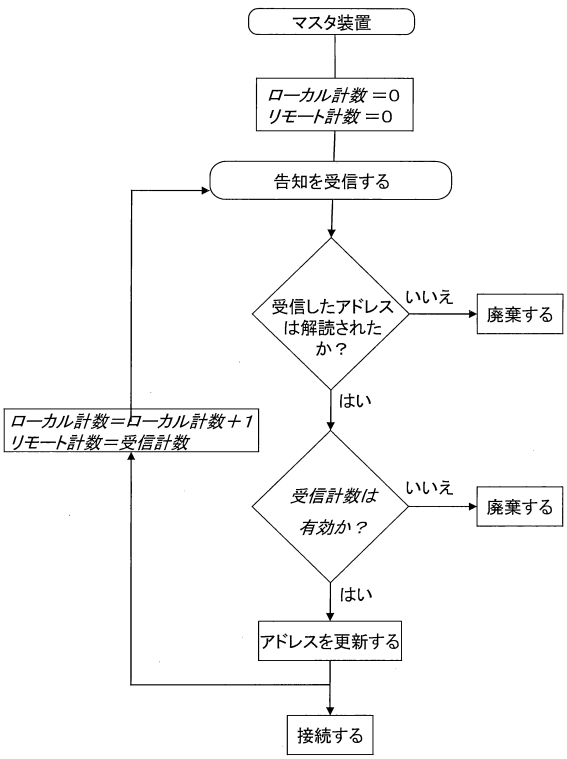
【図２】



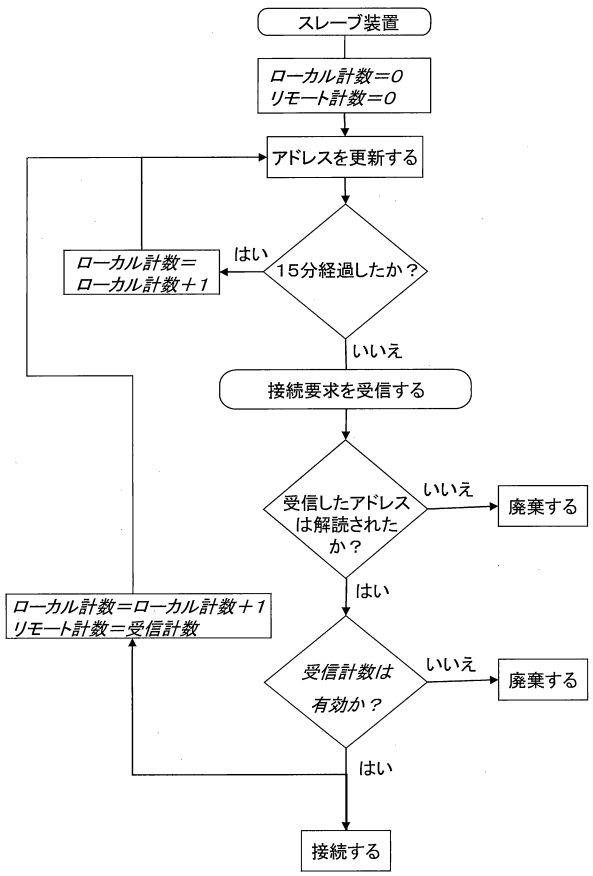

【図３】




【図４】




【図５】



フロントページの続き

審査官　金木　陽一

(56)参考文献　特開２００２－２１５０３０（ＪＰ，Ａ）
米国特許出願公開第２０１０／０３０３２３６（ＵＳ，Ａ１）
Core System Package [Host Volume], BLUETOOTH SPECIFICATION VERSION 4.0, ２０１０年　６月３０日, Vol. 3, pp. 344-359, 371-374, 600-601, [Retrieved on 2017-09-08.] Retrieved from the Internet, ＵＲＬ, https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｍ　１１／００
Ｈ０４Ｗ　１２／０２