【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成28年11月10日(2016.11.10)

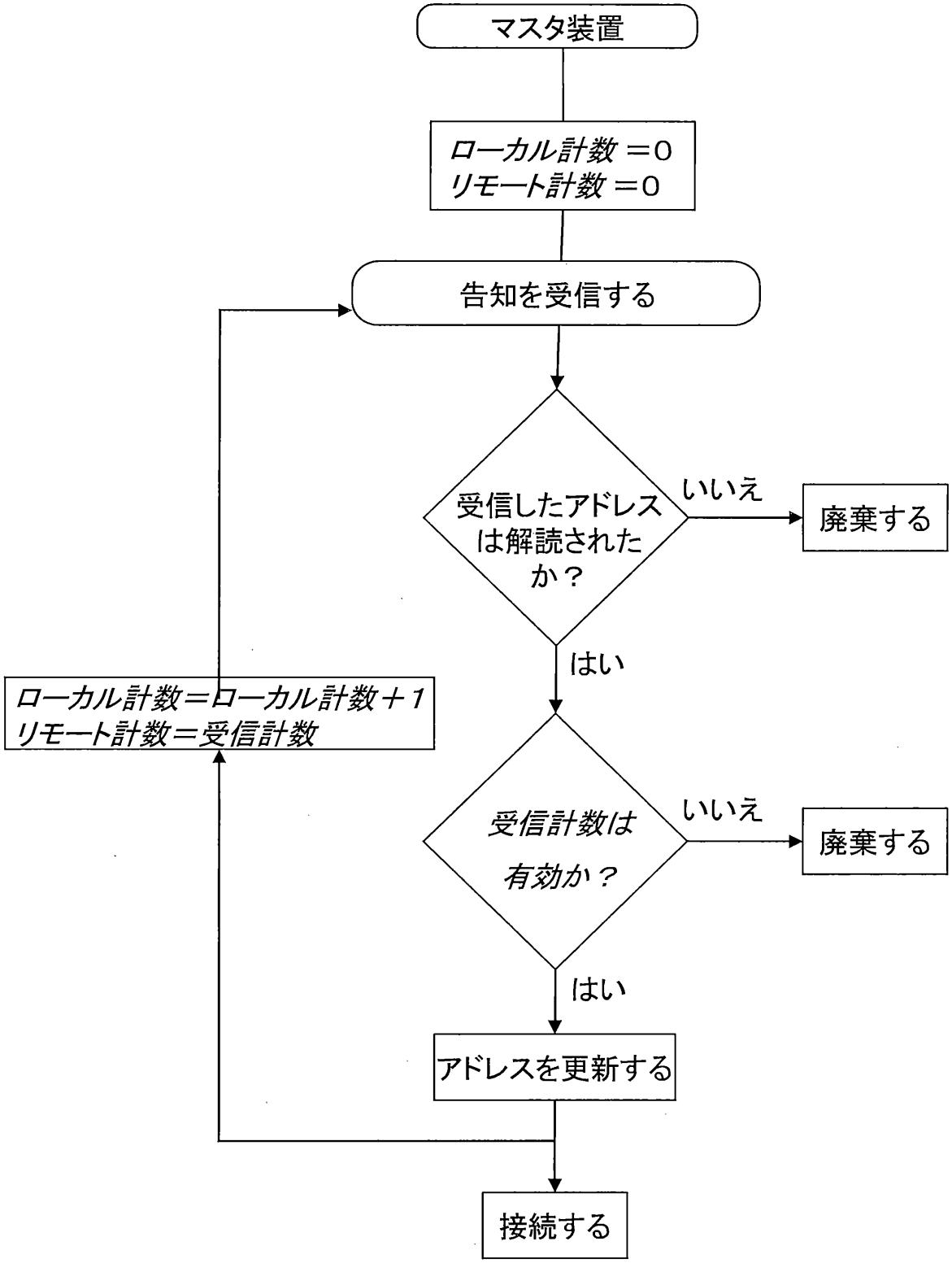
【公表番号】特表2016-504778(P2016-504778A)
【公表日】平成28年2月12日(2016.2.12)
【年通号数】公開・登録公報2016-010
【出願番号】特願2015-536059(P2015-536059)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｍ　11/00　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
Ｈ０４Ｗ　12/02　(2009.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７３Ｃ
Ｈ０４Ｍ　11/00　３０３
Ｇ０６Ｆ　21/44
Ｈ０４Ｗ　12/02

【手続補正書】
【提出日】平成28年9月16日(2016.9.16)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
連続した整数値で増分する計数器、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当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、
連続した整数値で増分するように構成されるか、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当す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）連続した整数値で増分するように構成されるか、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当する計数器の値と（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）連続した整数値で増分するように構成されるか、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当する計数器の値と（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）連続した整数値で増分するように構成されるか、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当する計数器の値と（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。

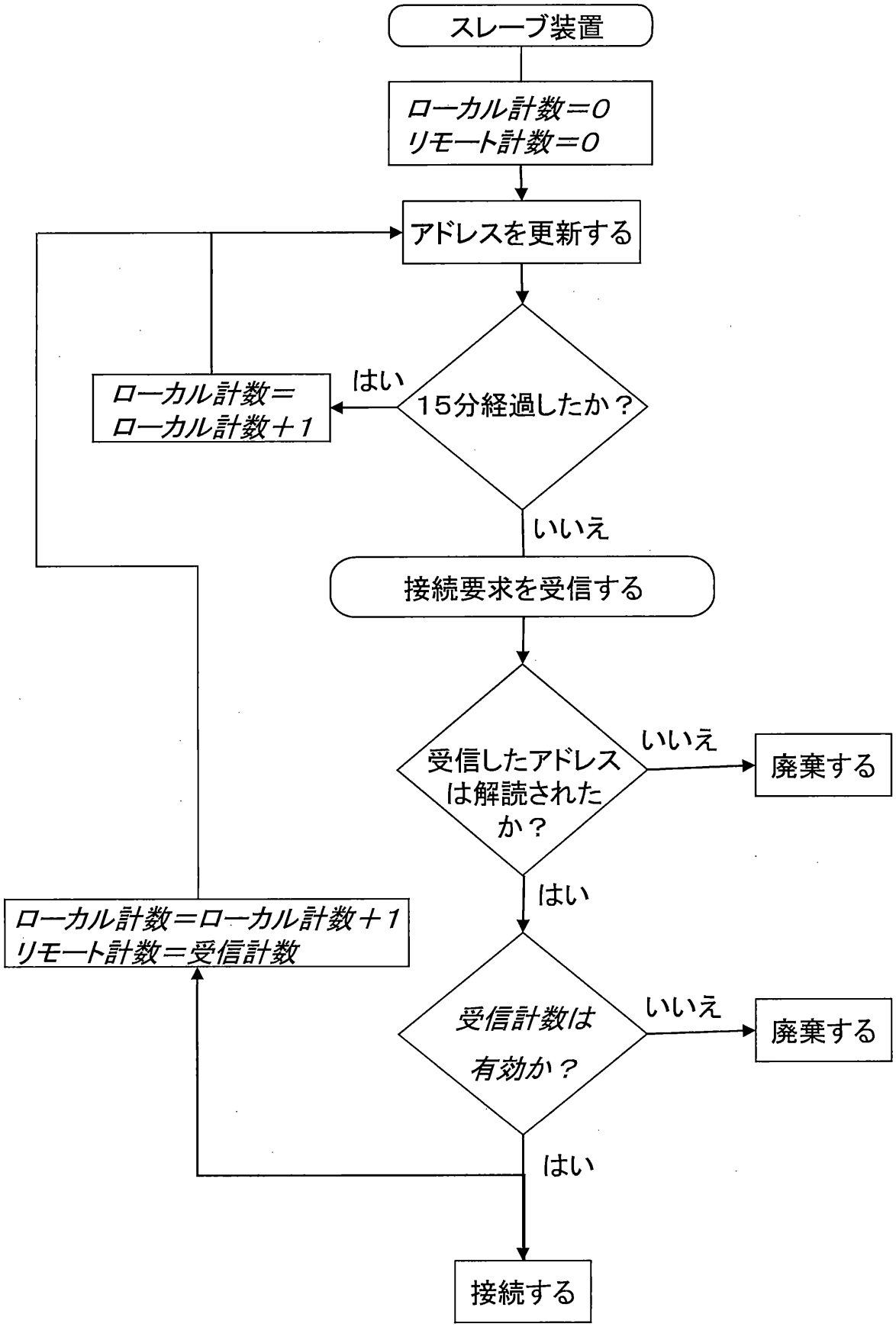
【請求項１４】
前記受信ハッシュが、前記受信値と、前記送信側無線装置と関係付けられた格納済身元解読キーとの組み合わせのハッシュであることを前記装置が判定することと、
前記受信値が所定の鮮度条件を満たしていることを前記装置が判定することと、をさらに含む
ことを特徴とする、請求項１３に記載の方法。
【請求項１５】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられた格納済ローカル計数値よりも大きいことを含む
ことを特徴とする、請求項１４に記載の方法。
【請求項１６】
前記鮮度条件は、前記受信値が、前記送信側無線装置と関係付けられたローカル計数値よりも大きい鮮度閾値量以下であることを含む
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）連続した整数値で増分するように構成されるか、または、線形フィードバックシフトレジスタ（ＬＦＳＲ）を有し前記ＬＦＳＲの連続する各出力が計数器増分に相当する計数器の値と（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。
【請求項２０】
前記受信値を、前記送信側無線装置と関係付けられたローカル計数値からローカルに生成された一連の前記ＬＦＳＲの値と比較するように構成される
ことを特徴とする、請求項１７乃至請求項１９のいずれか一項に記載の無線装置。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図４
【補正方法】変更
【補正の内容】

【図４】



【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図５
【補正方法】変更
【補正の内容】

【図５】


スレーブ装置
ローカル計数＝0
リモート計数＝0
アドレスを更新する
15分経過したか？
はい
ローカル計数＝
ローカル計数＋1
いいえ
接続要求を受信する
受信したアドレスは解読されたか？
いいえ
廃棄する
はい
受信計数は有効か？
いいえ
廃棄する
はい
ローカル計数＝ローカル計数＋1
リモート計数＝受信計数
接続する