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

特許第4883219号
(P4883219)

(45)発行日　平成24年2月22日(2012.2.22)　(24)登録日　平成23年12月16日(2011.12.16)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601C
H04L 9/14 (2006.01)　　H04L 9/00 641

請求項の数 5　(全 42 頁)

(21)出願番号　特願2010-509092 (P2010-509092)
(86)(22)出願日　平成21年4月24日 (2009.4.24)
(86)国際出願番号　PCT/JP2009/001903
(87)国際公開番号　WO2009/130917
(87)国際公開日　平成21年10月29日 (2009.10.29)
審査請求日　平成22年9月29日 (2010.9.29)
(31)優先権主張番号　特願2008-113530 (P2008-113530)
(32)優先日　平成20年4月24日 (2008.4.24)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(72)発明者　岩尾　忠重
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　増渕　健太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】ノード装置及びプログラム

(57)【特許請求の範囲】
【請求項１】
第１のノード装置と第２のノード装置を含む複数のノード装置によって構成されるネットワークの中の、前記第１のノード装置であって、
前記第１のノード装置に固有の暗号鍵である第１のアクセスキーを、第１の時間ごとに変更して生成するアクセスキー生成部と、
前記ネットワーク内の前記複数のノード装置で共通の共通鍵を、前記複数のノード装置で共通の時間である第２の時間ごとに変更して生成する共通鍵生成部と、
生成された前記第１のアクセスキーを、生成された前記共通鍵で暗号化して前記第２のノード装置に送信するアクセスキー通知部と、
前記第２のノード装置に固有の暗号鍵である第２のアクセスキーを前記共通鍵で暗号化したデータであるアクセスキー通知データを含む、前記第２のノード装置から送信されてきたアクセスキー通知フレームを、受信するアクセスキー受信部と、
前記アクセスキー通知データを、生成された前記共通鍵を用いて復号することにより、前記アクセスキー通知データから前記第２のアクセスキーを取得するアクセスキー復号化部と、
第１の平文フレームに、該第１の平文フレームから計算される第１のハッシュ値を含むデータを前記共通鍵で暗号化した第１の署名データを付与し、前記第１の署名データの付与された前記第１の平文フレームを、復号して得た前記第２のアクセスキーで暗号化して、第１の暗号化フレームとして送信するデータ送信部と、

第２のハッシュ値を含むデータを前記共通鍵で暗号化した第２の署名データが付与された、第２の平文フレームが、前記第１のアクセスキーにより暗号化された、第２の暗号化フレームを、前記第２のノード装置から受信するデータ受信部と、
前記第２の暗号化フレームを前記第１のアクセスキーで復号して、前記第２の暗号化フレームから、前記第２の署名データが付与された前記第２の平文フレームを得るデータ復号化部と、
生成された前記共通鍵を用いて前記第２の署名データを復号することにより前記第２のハッシュ値を取得し、前記第２の平文フレームから第３のハッシュ値を計算し、前記第２のハッシュ値と前記第３のハッシュ値との整合性が取れているか否かを確認する整合性確認部と
を有することを特徴とするノード装置。
【請求項２】
前記データ送信部は、前記第１の平文フレーム中に、前記第１の平文フレームを一意に識別するための第１の識別子と、第１の送信時刻を示す情報とを含ませ、
前記整合性確認部はさらに、前記データ復号化部が前記第２の暗号化フレームから復号した前記第２の平文フレームに含まれる第２の識別子が、過去に受信したことのある第３の暗号化フレームから復号した第３の平文フレームに含まれる第３の識別子と等しい場合に、前記第２の平文フレームと前記第３の平文フレームのうち、復号により得られる情報がより新しい送信時刻を示す方を破棄する
ことを特徴とする請求項１記載のノード装置。
【請求項３】
時刻同期フレームとして、前記第１のノード装置における第１の現在時刻と、前記第１のノード装置における時刻合わせを契機として取得した第１の同期時刻とを示すデータを含んだ第１の時刻同期フレームを生成して送信する時刻同期フレーム送信部と、
前記第２のノード装置における第２の現在時刻と、前記第２のノード装置における時刻合わせを契機として取得された第２の同期時刻とを示すデータを含む第２の時刻同期フレームを、前記第２のノード装置から受信する時刻同期フレーム受信部と、
前記第２の時刻同期フレームから得られる第２の同期時刻と、前記第１のノード装置が記憶している前記第１の同期時刻とを比較し、前記第２の同期時刻の方が新しければ、前記第２の現在時刻を前記第１のノード装置における現在時刻として設定して、前記第１のノード装置の時刻を更新する時刻更新部と、
前記時刻更新部が前記第１のノード装置の時刻を更新する際に、新たな第１の同期時刻として、前記第２の同期時刻を記憶する記憶部と
を有し、
前記共通鍵生成部は、前記時刻更新部が更新した時刻に基づいて前記第２の時間を計時する
ことを特徴とする請求項２記載のノード装置。
【請求項４】
第１のノード装置と第２のノード装置を含む複数のノード装置によって構成されるネットワークの中の、前記第１のノード装置が実行する方法であって、
前記第１のノード装置に固有の暗号鍵である第１のアクセスキーを、第１の時間ごとに変更して生成し、
前記ネットワーク内の前記複数のノード装置で共通の共通鍵を、前記複数のノード装置で共通の時間である第２の時間ごとに変更して生成し、
生成された前記第１のアクセスキーを、生成された前記共通鍵で暗号化して前記第２のノード装置に送信し、
前記第２のノード装置に固有の暗号鍵である第２のアクセスキーを前記共通鍵で暗号化したデータであるアクセスキー通知データを含む、前記第２のノード装置から送信されてきたアクセスキー通知フレームを、受信し、
前記アクセスキー通知データを、生成された前記共通鍵を用いて復号することにより、

前記アクセスキー通知データから前記第２のアクセスキーを取得し、
第１の平文フレームに、該第１の平文フレームから計算される第１のハッシュ値を含むデータを前記共通鍵で暗号化した第１の署名データを付与し、前記第１の署名データの付与された前記第１の平文フレームを、復号して得た前記第２のアクセスキーで暗号化して、第１の暗号化フレームとして送信し、
第２のハッシュ値を含むデータを前記共通鍵で暗号化した第２の署名データが付与された、第２の平文フレームが、前記第１のアクセスキーにより暗号化された、第２の暗号化フレームを、前記第２のノード装置から受信し、
前記第２の暗号化フレームを前記第１のアクセスキーで復号して、前記第２の暗号化フレームから、前記第２の署名データが付与された前記第２の平文フレームを得、
生成された前記共通鍵を用いて前記第２の署名データを復号することにより前記第２のハッシュ値を取得し、前記第２の平文フレームから第３のハッシュ値を計算し、前記第２のハッシュ値と前記第３のハッシュ値との整合性が取れているか否かを確認する
処理を前記第１のノード装置が実行する方法。
【請求項５】
第１のノード装置と第２のノード装置を含む複数のノード装置によって構成されるネットワークの中の、前記第１のノード装置を制御するコンピュータに、
前記第１のノード装置に固有の暗号鍵である第１のアクセスキーを、第１の時間ごとに変更して生成し、
前記ネットワーク内の前記複数のノード装置で共通の共通鍵を、前記複数のノード装置で共通の時間である第２の時間ごとに変更して生成し、
生成された前記第１のアクセスキーを、生成された前記共通鍵で暗号化して前記第２のノード装置に送信し、
前記第２のノード装置に固有の暗号鍵である第２のアクセスキーを前記共通鍵で暗号化したデータであるアクセスキー通知データを含む、前記第２のノード装置から送信されてきたアクセスキー通知フレームを、受信し、
前記アクセスキー通知データを、生成された前記共通鍵を用いて復号することにより、前記アクセスキー通知データから前記第２のアクセスキーを取得し、
第１の平文フレームに、該第１の平文フレームから計算される第１のハッシュ値を含むデータを前記共通鍵で暗号化した第１の署名データを付与し、前記第１の署名データの付与された前記第１の平文フレームを、復号して得た前記第２のアクセスキーで暗号化して、第１の暗号化フレームとして送信し、
第２のハッシュ値を含むデータを前記共通鍵で暗号化した第２の署名データが付与された、第２の平文フレームが、前記第１のアクセスキーにより暗号化された、第２の暗号化フレームを、前記第２のノード装置から受信し、
前記第２の暗号化フレームを前記第１のアクセスキーで復号して、前記第２の暗号化フレームから、前記第２の署名データが付与された前記第２の平文フレームを得、
生成された前記共通鍵を用いて前記第２の署名データを復号することにより前記第２のハッシュ値を取得し、前記第２の平文フレームから第３のハッシュ値を計算し、前記第２のハッシュ値と前記第３のハッシュ値との整合性が取れているか否かを確認する
処理を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、自律分散型のネットワークにおける、セキュリティ維持のための装置及びプログラムに関する。
【背景技術】
【０００２】
セキュリティ対策の一つとして、送信データを暗号化することが行われている。暗号化の方法としては、例えば共通鍵方式（対称鍵暗号方式ともいう）がある。また、さらにセ

キュリティを強固にするために、下記公知例のように共通鍵を一定時間ごとに変化させる技術がある。

【０００３】

また、ＷＥＰ（Wired Equivalent Privacy）、ＷＰＡ（Wi-Fi Protected Access）などのセキュリティ方式もある。

これらの技術によれば、サーバにおいて制御指示を出すことにより認証処理を行うのが一般的である。

【０００４】

また、通信システムにおいて、クライアント側の暗証番号については一定のまま、サーバの制御変数の変更のみで共有する暗号鍵を変更する技術も開示されている。これにより、短い時間間隔で共有する共通鍵を変化させ、暗号システムの安全性を向上させることができる。

【特許文献１】特開平９－３２１７４８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

有線か無線かを問わず、非常に多くのノード装置を含むネットワークを考えた場合、１つの管理サーバが共通鍵を生成（つまり時間に応じて変更）し、各ノード装置へ通知することは実用的ではない。すなわち、ノード装置の数が多いので、サーバから制御指示を送信するだけでも大変な負荷になってしまう。このため、各ノード装置が、暗号化のための動作を自律的に他のノード装置と協働して行うことが望ましい。

【０００６】

本発明は、暗号化のための動作を自律的に他のノード装置と協働して行うノード装置、及び、ノード装置に、暗号化のための動作を自律的に他のノード装置と協働して行うよう命令するプログラムを提供することを目的とする。

【課題を解決するための手段】

【０００７】

第１の態様のノード装置は、第１のノード装置と第２のノード装置を含む複数のノード装置によって構成されるネットワークの中の、前記第１のノード装置であって、アクセスキー生成部、共通鍵生成部、アクセスキー通知部、アクセスキー受信部、アクセスキー復号化部、データ送信部、データ受信部、データ復号化部及び整合性確認部を有する。

【０００８】

前記アクセスキー生成部は、前記第１のノード装置に固有の暗号鍵である第１のアクセスキーを、第１の時間ごとに変更して生成する。また、前記共通鍵生成部は、前記ネットワーク内の前記複数のノード装置で共通の共通鍵を、前記複数のノード装置で共通の時間である第２の時間ごとに変更して生成する。

【０００９】

前記アクセスキー通知部は、生成された前記第１のアクセスキーを、生成された前記共通鍵で暗号化して前記第２のノード装置に送信する。前記アクセスキー受信部は、前記第２のノード装置に固有の暗号鍵である第２のアクセスキーを前記共通鍵で暗号化したデータであるアクセスキー通知データを含む、前記第２のノード装置から送信されてきたアクセスキー通知フレームを、受信する。

【００１０】

前記アクセスキー復号化部は、前記アクセスキー通知データを、生成された前記共通鍵を用いて復号することにより、前記アクセスキー通知データから前記第２のアクセスキーを取得する。

【００１１】

前記データ送信部は、第１の平文フレームに、該第１の平文フレームから計算される第１のハッシュ値を含むデータを前記共通鍵で暗号化した第１の署名データを付与する。そして、前記データ送信部は、前記第１の署名データの付与された前記第１の平文フレーム

を、復号して得た前記第２のアクセスキーで暗号化して、第１の暗号化フレームとして送信する。

【００１２】

前記データ受信部は、第２の暗号化フレームを、前記第２のノード装置から受信する。ここで、前記第２の暗号化フレームとは、第２のハッシュ値を含むデータを前記共通鍵で暗号化した第２の署名データが付与された、第２の平文フレームが、前記第１のアクセスキーにより暗号化されたものである。

【００１３】

前記データ復号化部は、前記第２の暗号化フレームを前記第１のアクセスキーで復号して、前記第２の暗号化フレームから、前記第２の署名データが付与された前記第２の平文フレームを得る。

【００１４】

前記整合性確認部は、生成された前記共通鍵を用いて前記第２の署名データを復号することにより前記第２のハッシュ値を取得する。そして、前記整合性確認部は、前記第２の平文フレームから第３のハッシュ値を計算し、前記第２のハッシュ値と前記第３のハッシュ値との整合性が取れているか否かを確認する。

【００１５】

第２の態様のプログラムは、第１のノード装置と第２のノード装置を含む複数のノード装置によって構成されるネットワークの中の、前記第１のノード装置を制御するコンピュータにより実行されるプログラムである。前記プログラムは、第１の態様の前記第１のノード装置と同様に第２の態様の前記第１のノード装置が動作するよう、第２の態様の前記第１のノード装置を前記コンピュータに制御させるプログラムである。

【発明の効果】

【００１６】

上記いずれの態様においても、ネットワークの中の第１のノード装置は、自律的に、かつ、第２のノード装置などの他のノード装置と協働して、暗号化通信のための動作をすることが可能である。したがって、上記いずれの態様においても、複数のノード装置を含むネットワークにおける通信のセキュリティを高めることが可能となる。

【図面の簡単な説明】

【００１７】

【図１】アドホック通信システムの全体概念図である。

【図２】複数のノード装置を含むセンサネットワークの例を示すネットワーク構成図である。

【図３】実施形態に係るノード装置の構成図である。

【図４】実施形態に係るノード装置のハードウェア構成図である。

【図５】本実施形態に係るノード装置の構成をより詳細に示す図である。

【図６】実施形態に係るノード装置による認証方法を説明する図である。

【図７】２つのノード装置間で互いに相手のノード装置を認証して通信を行う処理を示したシーケンス図である。

【図８】データフレームのフォーマットを示す図である。

【図９】共通鍵更新処理のフローチャートである。

【図１０】アクセスキー更新処理のフローチャートである。

【図１１】ハローフレーム送信処理のフローチャートである。

【図１２】ハローフレームのフォーマットと、ハローフレームに関して行われる各種処理を説明する図である。

【図１３】ハローフレーム受信処理のフローチャートである。

【図１４】データフレーム送信処理のフローチャートである。

【図１５】データフレームのフォーマットと、データフレームに関して行われる各種処理の第１の例を説明する図である。

【図１６】データフレーム受信処理のフローチャートである。

【図１７】データフレームのフォーマットと、データフレームに関して行われる各種処理の第２の例を説明する図である。
【図１８】時刻の同期方法を説明する図である。
【図１９】時刻の同期方法を説明するシーケンス図である。
【図２０】時刻同期フレーム送信処理のフローチャートである。
【図２１】時刻同期フレーム受信処理のフローチャートである。
【発明を実施するための形態】
【００１８】
以下、本発明の実施の形態について、図面を参照して詳細に説明する。
図１は、アドホック通信システムの全体概念図である。図１に示すように、ノード装置（ａ、ｂ、…、ｓ、ｔ）が互いに接続されて網を構成している。アドホック通信システムにおいては、各ノード装置が中継器として動作し、スタートノード（図１の例ではノード装置ｂ）からゴールノード（図１の例ではノード装置ｔ）へと情報を伝達する。
【００１９】
各ノード装置は、それぞれ固有の識別情報（ＩＤ、Identification）であるノードＩＤを保有する。ＭＡＣ（Media Access Control）アドレスがノードＩＤとして利用されてもよい。
【００２０】
各ノード装置は、互いに隣接しているノード装置やネットワーク全体については把握していない。初期状態においては、互いのリンクは存在しておらず、各ノード装置は、自身以外のノード装置については把握していない。
【００２１】
そこで、図１に示すアドホック通信システムにおいて、スタートノードであるノード装置ｂから、ゴールノードであるノード装置ｔへと情報を伝達するには、まず、経路を決定する必要がある。経路を決定する手順は、以下のとおりである。
【００２２】
まず、各ノード装置は周囲のノード装置を検出する。そのために各ノード装置は、自身の存在を、近隣に存在するノード装置に周期的に通知する。近隣のノード装置への通知には、経路作成に関連した情報が付随している。各ノード装置は、他のノード装置から通知を受信すると、周囲のノード装置についてリストを作成して、自ノード装置の周囲に存在する他のノード装置を把握することができる。
【００２３】
周囲のノード装置を検出したノード装置は、作成したリストに基づいて、自ノード装置が情報を転送するノード装置を決定して、その決定したノード装置に情報を転送する。
各ノード装置は、セキュリティ対策のため、フレームを暗号化して相手のノード装置と通信を行う。具体的には、各ノード装置は、通信相手のノード装置に固有の暗号鍵と、ネットワーク内のノード装置間で共通の共通鍵とを用いて暗号化を行って、情報を通信相手のノード装置に送信する。また、各ノード装置は、通信相手のノード装置から情報を受信すると、自ノード装置に固有の暗号鍵と、上記の共通鍵とを用いてフレームを復号して情報を取り出す。
【００２４】
以後同様に、ノード装置間の通信においては、各ノード装置は、復号して得た暗号鍵を用いて通信相手のノード装置にデータの送信を行う。また、各ノード装置は、受信したデータが自ノード装置の生成した暗号鍵により暗号化されていることをもって、通信相手のノード装置を正当と判断する。
【００２５】
以下、本実施形態に係るノード装置による認証処理及び通信の方法について、具体的に説明する。
本実施形態のノード装置は、図１のような任意のアドホック通信システムにおいて利用可能であるが、例えば、図２のような、アドホックネットワークにより実現されるセンサ

ネットワークにおいて利用されてもよい。

【００２６】

図２は、複数のノード装置を含むセンサネットワークの例を示すネットワーク構成図である。

図２のセンサネットワークでは、複数のノード装置１Ａ～１Ｉ及びゲートウェイ装置ＧＷがアドホックネットワークを構成している。また、ゲートウェイ装置ＧＷは、例えばケーブルでサーバＳＶに接続されている。もちろん、ゲートウェイ装置ＧＷとサーバＳＶの間の接続は、ネットワークを介した接続でもよいし、無線による接続でもよい。

【００２７】

図２において、複数のノード装置１Ａ～１Ｉのそれぞれは、不図示の１つ以上のセンサと接続されているか、又は不図示の１つ以上のセンサを内蔵している。以下では説明の簡単化のため、各ノード装置１Ａ～１Ｉは、それぞれ１つのセンサと接続されているものとする。センサは、例えば、温度、圧力、加速度などを感知するセンサでもよい。また、異なる種類の複数のセンサが使われてもいてもよい。

【００２８】

各ノード装置１Ａ～１Ｉは、センサが感知した結果を表すデータ（以下「センサデータ」という）を、自ノード装置に接続されたセンサから取得する。そして、各ノード装置１Ａ～１Ｉは、取得したセンサデータを含む暗号化フレーム（以下「センサデータフレーム」という）を生成し、アドホックネットワークを通じてゲートウェイ装置ＧＷにセンサデータフレームを送信する。

【００２９】

例えば、各センサは、１分に１回センサデータをノード装置に出力してもよい。したがって、上記のとおりノード装置１Ａ～１Ｉがそれぞれ１つのセンサと接続されている場合、各ノード装置１Ａ～１Ｉは、１分間に１回センサデータフレームを送信することになる。

【００３０】

ゲートウェイ装置ＧＷは、各ノード装置１Ａ～１Ｉと同様に後述の図３の各部を備えており、ノード装置１Ａ～１Ｉと協働して自律的にアドホックネットワークを構築することができる。つまり、ノード装置１Ａ～１Ｉとゲートウェイ装置ＧＷの間で、共通鍵は共通しており、後述の時刻同期用の固定鍵も共通している。

【００３１】

ゲートウェイ装置ＧＷは、各ノード装置１Ａ～１Ｉから送信されてきたセンサデータフレームに含まれるセンサデータをサーバＳＶに送信する。例えば、ゲートウェイ装置ＧＷは、次のように動作してもよい。

【００３２】

ゲートウェイ装置ＧＷは、受信したセンサデータフレームを復号してセンサデータを抽出する。そして、ゲートウェイ装置ＧＷは、抽出したセンサデータを含むデータを、サーバＳＶに送信する。

【００３３】

あるいは、ゲートウェイ装置ＧＷは、受信したセンサデータフレームから、センサデータフレームの送信元のノード装置（１Ａ～１Ｉのいずれか）の識別情報をさらに抽出してもよい。そして、ゲートウェイ装置ＧＷは、センサデータと識別情報を含むデータを暗号化したデータをペイロードに含む暗号化フレームを生成して、サーバＳＶに送信してもよい。

【００３４】

サーバＳＶは、センサが感知する物理量に基づく任意の各種の処理を、収集したセンサデータを使って行うことができる。例えば、各センサが温度センサの場合、サーバＳＶは、温度分布や温度変化を調べる処理を行ってもよいし、温度予測処理を行ってもよい。

【００３５】

以下に詳しく説明する本実施形態のノード装置１を、図２のノード装置１Ａ～１Ｉとし

て利用すれば、サーバＳＶは、センサデータを秘密状態に保ちつつ収集することができ、さらに、改竄されていない正しいセンサデータを収集することができる。

【００３６】

図３は、本実施形態に係るノード装置の構成図である。図３に示すノード装置１は、アクセスキー生成部２、共通鍵生成部３、暗号化部４、復号化部５、フレーム処理部６、送信部７、受信部８及び時刻同期部９を有する。例えば、図２のノード装置１Ａ～１Ｉの各々は、図３のような構成を有する。

【００３７】

アクセスキー生成部２は、ノード装置１に固有の暗号鍵（以下「アクセスキー」という）を生成する。アクセスキーは、公知のＷＥＰやＷＰＡ等の技術を用いて生成される。アクセスキーは、対称鍵暗号方式における暗号鍵として生成され、使用される。

【００３８】

また、アクセスキーは、所定の時間間隔t_1でランダムに更新される。本実施形態では、例えば、t_1＝１０（分）である。

なお、アクセスキーは、ＲＣ４（Rivest's Cipher 4）により暗号化されて他のノード装置に送信され、本実施形態では、アクセスキーの長さは１２８ビットである。ＲＣ４はストリーム暗号の１種なので、ＲＣ４によって暗号化された暗号文（ciphertext）の長さは、元の平文（plaintext）の長さと等しい。

【００３９】

ところで、一般に、鍵の長さが６４ビットのＲＣ４の解読には５０万フレームを、鍵の長さが１２８ビットの解読には１００万フレームを収集することが必要であると言われている。これに対し、上記のとおり、本実施形態では、アクセスキーはt_1＝１０分ごとにランダムに変化する。

【００４０】

例えば、図２に関して例示したように、フレームが通常毎分１フレーム送信されるとすると、１０分間では１０フレーム送信されることとなる。そして、例えば、図２の例では、センサデータフレームの最終的な宛先であるゲートウェイ装置ＧＷが、アドホックネットワーク内で最も多くのフレームを受信することになる。しかし、ゲートウェイ装置ＧＷであっても、例えば総数５００台のノード装置からデータを受信する場合のフレーム数は、１分間あたり約５００フレームである。すなわち、アクセスキーが更新されるまでの１０分間に、不正ノード装置が解読に必要なフレームを収集することは、事実上不可能であると言うことができる。

【００４１】

共通鍵生成部３は、ノード装置１内に備えられた耐タンパデバイス（例えば後述の図４の耐タンパ性ＰＩＣマイコン１４）等により、図１のネットワーク内のノード装置で共通する暗号鍵である共通鍵を生成する。共通鍵は、所定の時間間隔t_2で更新される。本実施形態では、例えば、t_2＝１２（時間）である。

【００４２】

各ノード装置において保有する時刻情報は、ネットワーク内で同期されている。このため、共通鍵は、時間により変化するが、ある時刻においては、ネットワーク内のノード装置で共通する。

【００４３】

暗号化部４は、他のノード装置に送信するフレームに含まれるデータの暗号化を行い、復号化部５は、他のノード装置から暗号化して送信されたフレームに含まれるデータの復号を行う。

【００４４】

送信部７は、図３に示すノード装置１において生成した暗号化データを含む暗号化フレームを、他のノード装置に向けて送信し、受信部８は、他のノード装置から送信された暗号化フレームを受信する。

【００４５】

フレーム処理部６は、受信したフレームの処理を実行する。例えば、フレーム処理部６は、受信したフレームの所定のフィールドから情報を取り出して、「既に受信したフレームであるか否か」の判断を、上記「受信したフレームの処理」として行ってもよい。あるいは、フレーム処理部６は、受信したフレームの所定のフィールドから情報を取り出して、「正当なノード装置から送信されたフレームであるか否か」の判断等を、上記「受信したフレームの処理」として行ってもよい。

【００４６】

フレーム処理部６はさらに、送信するフレームを作成する処理も行う。

時刻同期部９は、図３に示すノード装置１において保有する時刻を、ネットワーク内の他のノード装置の時刻と同期させるための処理を実行する。時刻同期部９の動作の詳細は、図１８～図２１とともに後述する。

【００４７】

図３に示すノード装置１は、ネットワーク内の他のノード装置と通信を開始する前に、相手のノード装置との間で、共通鍵を用いて暗号化したアクセスキーを交換する。共通鍵により暗号化されたアクセスキーは、例えば「ハローフレーム」と呼ばれる所定の形式のフレームの所定のフィールドに格納されて相手のノード装置に送信される。

【００４８】

なお、以下、説明の便宜上、ノード装置１自身が生成したアクセスキーを「内部由来（internally-originated）アクセスキー」と称し、他のノード装置から受け取ったアクセスキーを「外部由来（externally-originated）アクセスキー」と称することがある。

【００４９】

図３のノード装置１は、通信相手のノード装置（図３のノード装置１と同様の構成を有する不図示の第２のノード装置）から受信した、暗号化されたアクセスキーを、自ノード装置１において保有する共通鍵を用いて復号する。そして、図３のノード装置１は、以降、その不図示の第２のノード装置と通信を行う際には、復号により得られたアクセスキー（すなわち外部由来アクセスキー）を用いて、不図示の第２のノード装置宛のフレームの暗号化を行う。

【００５０】

上記のとおり、共通鍵及びアクセスキーはそれぞれ所定の時間間隔t_2及びt_1で更新されている。このため、第三者が不正にある時点での共通鍵あるいはアクセスキーを取得したとしても、なりすまし等の不正なアクセスは不可能となる。

【００５１】

続いて、図３の構成を実現するハードウェアの具体例について図４を参照して説明する。図４は、本実施形態に係るノード装置１のハードウェア構成図である。

図３のノード装置１は、ＭＰＵ（MicroProcessing Unit）１１と、有線ＰＨＹ（PHYsical layer）処理部１２と、タイマＩＣ（Integrated Circuit）１３と、耐タンパ性ＰＩＣ（Peripheral Interface Controller）マイコン（microcomputer）１４を備える。ノード装置１はさらに、ＤＲＡＭ（Dynamic Random Access Memory）１５と、フラッシュメモリ１６と、無線ＬＡＮ（Local Area Network）処理部１７を備える。

【００５２】

ＭＰＵ１１と有線ＰＨＹ処理部１２の間の接続インタフェイスは、例えば、ＭＩＩ（Media Independent Interface）／ＭＤＩＯ（Management Data Input/Output）１８である（なお「ＭＩＩ／ＭＤＩＯ」は「ＭＩＩ又はＭＤＩＯ」の意味である）。ＭＩＩとＭＤＩＯはいずれも、物理層とＭＡＣ副層（Media Access Control sublayer）との間のインタフェイスである。

【００５３】

また、タイマＩＣ１３と耐タンパ性ＰＩＣマイコン１４は、I^2C（Inter-Integrated Circuit）／ＰＩＯ（Parallel Input/Output）バス１９によりＭＰＵ１１と接続されている（なお「I^2C／ＰＩＯバス」は「I^2Cバス又はＰＩＯバス」の意味である）。

【００５４】

ＤＲＡＭ１５とフラッシュメモリ１６と無線ＬＡＮ処理部１７は、ＰＣＩ（Peripheral Component Interconnect）バス２０によりＭＰＵ１１と接続されている。

ＭＰＵ１１は、不揮発性記憶装置の１種であるフラッシュメモリ１６上に格納されたファームウェアなどの種々のプログラムをＤＲＡＭ１５上にロードして実行することで様々な処理を実行する。ＭＰＵ１１は、例えば、耐タンパ性ＰＩＣマイコン１４のドライバや、後述の各種処理をノード装置１に実行させるためのファームウェアプログラムなど、種々のプログラムを実行する。

【００５５】

なお、ＤＲＡＭ１５には、暗号化鍵などの各種のデータが格納されてもよい。また、ＤＲＡＭ１５は、フレームの送信バッファ及び受信バッファとしても使われる。フラッシュメモリ１６は、上記のとおり、ファームウェアプログラムなどを格納する。また、フラッシュメモリ１６には、ノード装置１自身に固有の情報（例えば、ノードＩＤやＭＡＣアドレス）も格納されている。

【００５６】

有線ＰＨＹ処理部１２は、有線接続における物理層の処理を行う回路である。また、無線ＬＡＮ処理部１７は、無線ＬＡＮ接続における物理層の処理を行うハードウェアである。無線ＬＡＮ処理部１７は、例えばアンテナ、ＡＤＣ（Analog-to-Digital Converter）、ＤＡＣ（Digital-to-Analog Converter）、変調器、復調器などを含み、物理層とＭＡＣ副層の処理を行う。したがって、本実施形態では、ノード装置１が、有線通信と無線通信の双方を行うことができる。しかし、ノード装置１が、有線通信又は無線通信の一方のみを行う実施形態も可能である。

【００５７】

タイマＩＣ１３は、設定された時間が経過するまでカウントアップ動作を行い、設定された時間が経過すると割り込み信号を出力する回路である。

耐タンパ性ＰＩＣマイコン１４は、共通鍵を生成する所定のアルゴリズムが組み込まれたマイコンである。耐タンパ性ＰＩＣマイコン１４は耐タンパ性なので、共通鍵を生成する所定のアルゴリズムが具体的にどのようなアルゴリズムであるかは、外部から解析することができない。

【００５８】

続いて、図３と図４を参照して説明したノード装置１の構成について、図５を参照してさらに詳しく説明する。図５は、本実施形態に係るノード装置１の構成をより詳細に示す図である。

【００５９】

図５には、図３と同様のアクセスキー生成部２、共通鍵生成部３、暗号化部４、復号化部５、フレーム処理部６、送信部７、受信部８及び時刻同期部９が示されている。

図５に示すように、受信部８は、ノード装置１が受信したフレームをフレームの種類に応じて分類するフレーム分岐処理部２１と、フレームの種類別の受信バッファを備える。受信バッファは、例えば図４のＤＲＡＭ１５により実現される。

【００６０】

具体的に本実施形態では、ハローフレーム、時刻同期フレーム及びデータフレームという３つの種類に対応して、ハローフレーム受信バッファ２２と、時刻同期フレーム受信バッファ２３と、データフレーム受信バッファ２４とを、受信部８が備えている。

【００６１】

フレーム分岐処理部２１は、例えば、図４の無線ＬＡＮ処理部１７とＭＰＵ１１により、又は有線ＰＨＹ処理部１２とＭＰＵ１１により、実現される。図１２、図１５及び図１７とともに後述するように、フレームのヘッダにはフレームの種類を示す「フレームタイプ」フィールドが含まれるので、フレーム分岐処理部２１は、フレームタイプフィールドの値に基づいて、受信したフレームの種別を認識し、受信したフレームの分類を行うことができる。

【００６２】

また、復号化部５は、３つのフレームの種類に対応して、ハローフレーム復号化部２５と、時刻同期フレーム復号化部２６と、データフレーム復号化部２７とを備える。復号化部５は、本実施形態ではＭＰＵ１１により実現されるが、専用のハードウェア回路により実現されてもよい。

【００６３】

ハローフレーム復号化部２５は、ハローフレーム受信バッファ２２に格納されたハローフレームを復号して、図４には不図示の他のノード装置のアクセスキーを抽出して出力する。時刻同期フレーム復号化部２６は、時刻同期フレーム受信バッファ２３に格納された時刻同期フレームを復号し、復号して得られた情報を時刻同期部９に出力する。データフレーム復号化部２７は、データフレーム受信バッファ２４に格納されたデータフレームを復号する。

【００６４】

さらに、ノード装置１は、図５に図示の、他のノード装置用のアクセスキー（すなわち外部由来アクセスキー）を格納するアクセスキー格納部２８を備える。アクセスキー格納部２８には、ハローフレーム復号化部２５で復号された平文に含まれる外部由来アクセスキーが格納される。より具体的には、アクセスキー格納部２８は、複数のノード装置それぞれに対応する外部由来アクセスキーを、複数のノード装置を識別する情報（例えばノードＩＤ又はＭＡＣアドレスなど）と対応付けて格納している。

【００６５】

なお、アクセスキー格納部２８は、例えば図４のＤＲＡＭ１５によって実現され、また、少なくとも一部がＭＰＵ１１内のキャッシュメモリによって実現されてもよい。

また、ノード装置１は、復号されたデータフレームの正しさを確認する確認部２９を含む。確認部２９の動作の詳細は、図１６とともに後述するが、確認部２９は例えばＭＰＵ１１により実現される。なお、本実施形態では、確認部２９は、復号されたアクセスキーの正しさの確認も行う。

【００６６】

また、フレーム処理部６は受信データフレーム処理部３０を含み、確認部２９により「正しい（すなわち改竄されていない）」と確認されたデータフレームを使った処理を行う。例えば、受信データフレーム処理部３０は、既に受信したデータフレームと同一のデータフレームを再度受信したのか、新たなデータフレームを受信したのかを判別する処理を行ってもよい。受信データフレーム処理部３０も、ＭＰＵ１１により実現することができる。

【００６７】

なお、上記のデータフレーム復号化部２７における復号では、ノード装置１自身のアクセスキーが使われる。そのため、ノード装置１は、自ノード装置１用のアクセスキー（すなわち内部由来アクセスキー）を格納するアクセスキー格納部３１をさらに備えている。アクセスキー格納部３１は、例えばＤＲＡＭ１５によって実現されてもよく、ＭＰＵ１１内のキャッシュメモリによって実現されてもよい。

【００６８】

他方、上記のハローフレーム復号化部２５における復号では、ネットワーク内の複数のノード装置で共通の共通鍵が使われる。そのため、ノード装置１は、共通鍵を格納する共通鍵格納部３２をさらに備えている。共通鍵格納部３２も、例えばＤＲＡＭ１５によって実現されてもよく、ＭＰＵ１１内のキャッシュメモリによって実現されてもよい。

【００６９】

また、共通鍵格納部３２に格納される共通鍵は、図３に関して説明したように、共通鍵生成部３によって生成される。すなわち、本実施形態によれば、複数のノード装置間で共通鍵を交換する必要がないように、複数のノード装置それぞれの共通鍵生成部３において、同じアルゴリズムにしたがって時刻から一意に決まる共通鍵が生成される。

【００７０】

なお、共通鍵の漏洩を防ぐため、本実施形態の共通鍵生成部３は、図４の耐タンパ性Ｐ

ＩＣマイコン１４によって実現される。すなわち、共通鍵生成部３は耐タンパ性である。
また、共通鍵生成部３は、共通鍵を生成するために時刻情報を利用する。具体的には、ノード装置１は時計３３を備えており、共通鍵生成部３は時計３３を参照して時刻情報を得る。

【００７１】
なお、詳しくは図１０とともに後述するが、ノード装置１はさらに、図４のタイマＩＣ１３により実現されるカウンタ３４を備えている。カウンタ３４はカウントアップ動作を繰り返し、カウンタ３４の値が予め設定された値に達すると、アクセスキー生成部２がアクセスキーを生成し、カウンタ３４がクリアされる。

【００７２】
また、上記の時刻同期フレーム復号化部２６における復号では、ネットワーク内の複数のノード装置で共通しており、時間によって変動することもない、固定された時刻同期鍵が使われる。そのため、ノード装置１は、時刻同期鍵を格納する時刻同期鍵格納部３５をさらに備えている。

【００７３】
時刻同期鍵は、例えば、ＭＰＵ１１が実行するファームウェアプログラムに定数として予め書き込まれており、ファームウェアプログラムがＤＲＡＭ１５にロードされることで、ＤＲＡＭ１５に記憶されてもよい。時刻同期鍵格納部３５は、例えば、フラッシュメモリ１６、ＤＲＡＭ１５又はＭＰＵ１１内のキャッシュメモリによって実現することができる。

【００７４】
ところで、フレーム処理部６は、受信したデータフレームを処理する上記の受信データフレーム処理部３０だけではなく、ハローフレームを作成するハローフレーム作成部３６をさらに備えている。ハローフレーム作成部３６は、アクセスキー格納部３１からノード装置１自身のアクセスキーを読み出し、ハローフレームの元となる平文フレームを作成し、出力する。ハローフレーム作成部３６は、例えば、ＭＰＵ１１により実現される。

【００７５】
ハローフレーム作成部３６から出力される平文フレームは、暗号化部４に入力され、暗号化される。なお、暗号化部４は、ハローフレーム暗号化部３７、時刻同期フレーム暗号化部３８及びデータフレーム暗号化部３９を備え、暗号化部４内のこれら各部も、例えばＭＰＵ１１により実現される。

【００７６】
ハローフレーム暗号化部３７は、共通鍵格納部３２に格納されている共通鍵を用いて、ハローフレームの元となる平文フレームを暗号化する。また、時刻同期フレーム暗号化部３８は、時刻同期鍵格納部３５に格納されている時刻同期鍵を用いて、時刻同期フレームの元となる平文フレームを暗号化する。そして、データフレーム暗号化部３９は、アクセスキー格納部２８に格納されているアクセスキーのうち、データフレームの宛先のノード装置用のアクセスキーを用いて、データフレームの元となる平文フレームを暗号化する。

【００７７】
なお、時刻同期フレームの元となる平文フレームは、詳しくは図２０とともに後述するとおり、時刻同期部９から時刻同期フレーム暗号化部３８に出力される。
また、フレーム処理部６はさらに、データフレームの元となる平文フレームを作成してデータフレーム暗号化部３９に出力するデータフレーム作成部４０も備えている。

【００７８】
暗号化部４内で暗号化された各種フレームは送信部７に出力され、ノード装置１から送信される。具体的には、送信部７は、例えば図４のＤＲＡＭ１５によって実現される３つのバッファ（すなわち、ハローフレーム送信バッファ４１と時刻同期フレーム送信バッファ４２とデータフレーム送信バッファ４３）と、さらに送信処理部４４とを備える。送信処理部４４は、例えば有線ＰＨＹ処理部１２とＭＰＵ１１により実現されてもよいし、無線ＬＡＮ処理部１７とＭＰＵ１１により実現されてもよい。

【００７９】
ハローフレーム送信バッファ４１は、暗号化されたハローフレームをハローフレーム暗号化部３７から受け取って格納し、送信処理部４４に出力する。時刻同期フレーム送信バッファ４２は、暗号化された時刻同期フレームを時刻同期フレーム暗号化部３８から受け取って格納し、送信処理部４４に出力する。データフレーム送信バッファ４３は、暗号化されたデータフレームをデータフレーム暗号化部３９から受け取って格納し、送信処理部４４に出力する。そして、送信処理部４４は、受け取ったフレームを送信する。
【００８０】
なお、図５に示すように、ノード装置１はさらに、例えばＤＲＡＭ１５によって実現される最新送信時刻格納部４５を備えるが、最新送信時刻格納部４５については図１６とともに後述するので、ここでは説明を省略する。
【００８１】
以上、図３～図５を参照してノード装置１の構成について説明したので、続いて、ノード装置１の動作について図６～図２１を参照して説明する。
図６は、本実施形態に係るノード装置１による認証方法を説明する図である。
【００８２】
図６に示すように、ノード装置１Ａの周辺にノード装置１Ｂ及びノード装置１Ｃが存在する場合に、ノード装置１Ａは、生成したアクセスキーａ１を、それぞれノード装置１Ｂ及びノード装置１Ｃのアクセスキーｂ１及びｃ１と交換する。そして、ノード装置１Ａは、ノード装置１Ｂに対しては、アクセスキーｂ１によりデータフレームを暗号化して送信し、ノード装置１Ｃに対しては、アクセスキーｃ１によりデータフレームを暗号化して送信する。
【００８３】
図６の例では、ノード装置１Ａにとっては、アクセスキーａ１は内部由来アクセスキーであり、アクセスキーｂ１とｃ１は外部由来アクセスキーである。他方で、ノード装置１Ｂにとっては、アクセスキーａ１は外部由来アクセスキーであり、アクセスキーｂ１が内部由来アクセスキーである。
【００８４】
ノード装置１Ａは、ノード装置１Ｂとノード装置１Ｃとでそれぞれ異なるアクセスキー（ｂ１及びｃ１）を使用する。また、例えば、ノード装置１Ｂとの通信において、ノード装置１Ａは、データ送信時にはアクセスキーｂ１を使用するが、データ受信時にはアクセスキーａ１を使用する。このように、ノード装置１Ａは、データ送信時とデータ受信時とでそれぞれ異なるアクセスキーを使用して通信を行う。換言すれば、内部由来アクセスキーは復号化用の鍵であり、外部由来アクセスキーは暗号化用の鍵である。
【００８５】
このように、アドホック通信ネットワークを構成するノード装置のそれぞれが、隣接するノード装置とアクセスキーを上記の方法により交換し、通信相手のノード装置から受信したアクセスキーを用いてフレームを暗号化して送信する。また、これとともに、通信相手から受信したフレームについては、自ノード装置において定期的に更新するアクセスキーを用いて復号する。これにより、セキュリティが確保される。
【００８６】
上記のとおり、本実施形態においては、ネットワーク内の各ノード装置が、隣接するノード装置と通信を行うときに、通信相手のノード装置が自ノード装置にアクセスするためのアクセスキーを生成する。そして、各ノード装置は、ネットワーク内で共通する共通鍵を用いて、上記の生成したアクセスキーを暗号化し、暗号化したアクセスキーをハローフレームでブロードキャストする。各ノード装置は、隣接ノード装置から受信したハローフレームに含まれるアクセスキーを共通鍵で復号し、復号で得たアクセスキーを用いて隣接ノード装置にアクセスする。以下、２台のノード装置間で実行される処理について具体的に説明する。
【００８７】

図７は、２つのノード装置間で互いに相手のノード装置を認証して通信を行う処理を示したシーケンス図である。ここでは、２台のノード装置１を互いに区別するために、それぞれを「ノード装置１Ａ」及び「ノード装置１Ｂ」とする。

【００８８】

まず、ステップＳ１で、ノード装置１Ａから通信相手ノード装置であるノード装置１Ｂに向けて、ノード装置１Ａで生成したアクセスキーａ１が送信される。アクセスキーａ１は、先述のとおり、ノード装置１Ａとノード装置１Ｂとの間で共通して保有する共通鍵により暗号化されている。ノード装置１Ｂは、自ノード装置１Ｂにおいて耐タンパデバイスを用いて生成した共通鍵を用いて、復号処理を行い、アクセスキーａ１を得る。

【００８９】

次に、ステップＳ２で、ノード装置１Ｂから通信相手ノード装置であるノード装置１Ａに向けて、ノード装置１Ｂで生成したアクセスキーｂ１が送信される。アクセスキーｂ１についても、ノード装置１Ａとノード装置１Ｂとの間で共通する共通鍵により暗号化されている。ノード装置１Ａは、自ノード装置１Ａにおいて耐タンパデバイスを用いて生成した共通鍵を用いて、復号処理を行い、アクセスキーｂ１を得る。

【００９０】

ステップＳ１及びステップＳ２の処理において、一方のノード装置が不正にアクセスしようとする第三者である場合には、通信相手ノード装置との間に共通する共通鍵を持たず、復号して通信相手ノード装置のアクセスキーを取得することができない。このことを利用して、２台のノード装置１Ａ、１Ｂの間でアクセスキーの交換ができた場合には、通信相手のノード装置１Ａ及び１Ｂを正当と判断することができる。つまり、ノード装置１Ａ、１Ｂの間でアクセスキーの交換ができた場合には、ノード装置１Ａはノード装置１Ｂを正当と判断し、ノード装置１Ｂはノード装置１Ａを正当と判断することができる。

【００９１】

本実施形態においては、通信相手ノード装置とのアクセスキーの交換の成否をもって通信相手ノード装置の認証を行うこととし、認証が成功した場合には、ステップＳ３以降の通信を開始する。

【００９２】

なお、ステップＳ１及びステップＳ２の認証処理は、アクセスキーが更新されるごとに行われる。

ステップＳ３で、ノード装置１Ａからノード装置１Ｂに向けて、データを含むフレームが送信される。送信されるフレームは、ステップＳ２においてノード装置１Ａが取得したアクセスキーｂ１により暗号化されている。例えば、図２に関して説明したように、センサデータを含む暗号化フレームであるセンサデータフレームが、ステップＳ３では送信される。

【００９３】

また、フレームには、署名がされている。署名については後述する。フレームを受信したノード装置１Ｂは、自ノード装置１Ｂにおいて生成したアクセスキーｂ１を用いて、受信したフレームの復号を行い、データを得る。

【００９４】

ステップＳ４で、ノード装置１Ｂからノード装置１Ａに向けて、データを含むフレームが送信される。送信されるフレームは、ステップＳ１においてノード装置１Ｂが取得したアクセスキーａ１により暗号化されており、署名がされている。フレームを受信したノード装置１Ａにおいては、自ノード装置１Ａにおいて生成したアクセスキーａ１を用いて、受信したフレームの復号を行い、データを得る。

【００９５】

図７に示すとおり、本実施形態に係るノード装置１（１Ａ及び１Ｂ）は、通信相手のノード装置（１Ｂ及び１Ａ）と共通する共通鍵を用いて、各ノード装置（１Ａ及び１Ｂ）において生成するアクセスキー（ａ１及びｂ１）を暗号化して交換する。通信相手のノード装置（１Ｂ及び１Ａ）が正当である場合には、通信相手のノード装置（１Ｂ及び１Ａ）は

、自ノード装置（１Ａ及び１Ｂ）はと共通する共通鍵を保有している。

【００９６】

このため、各ノード装置（１Ａ及び１Ｂ）は、通信相手のノード装置（１Ｂ及び１Ａ）から受信したアクセスキー（ｂ１及びａ１）を、自ノード装置（１Ａ及び１Ｂ）において保有する共通鍵を用いて復号することができる。不正にアクセスしようとする第三者においては上記共通鍵を保有していないため、各ノード装置（１Ａ及び１Ｂ）は、受信したアクセスキー（ｂ１及びａ１）を復号できるか否かにより、通信相手のノード装置（１Ｂ及び１Ａ）について正当か不当かを判断することができる。各ノード装置１は、通信相手のノード装置と定期的にアクセスキーを交換し、正当であると判断できたノード装置と通信を継続する。

【００９７】

また、データの受信時においては、自ノード装置において生成したアクセスキーを用いて復号処理を行い、データを取り出す。例えば、ステップＳ３では、受信側のノード装置１Ｂは、自ノード装置１Ｂが生成したアクセスキーｂ１を用いて復号処理を行う。

【００９８】

データの送信時においては、認証処理において通信相手ノード装置から受信した、通信相手ノード装置において生成されたアクセスキーを用いて暗号化して、データを送信する。例えば、ステップＳ３では、送信側のノード装置１Ａは、通信相手ノード装置１Ｂからステップ Ｓ２で受信したアクセスキーｂ１を用いて暗号化処理を行う。

【００９９】

図８は、データフレームのフォーマットを示す図である。フォーマットの更なる詳細は、図１５及び図１７とともに後述する。また、ハローフレームのフォーマットの例は図１２とともに後述する。

【０１００】

図８に示すように、データフレームは、ヘッダ、フレームの識別情報（ＦＩＤ）、時刻情報及びボディからなり、データフレームには署名が追加されている。

ヘッダには、フレームの宛先情報等が格納される。ＦＩＤには、送信元のノード装置１が付与した、データフレームを識別するためのシーケンス番号等が格納される。時刻情報には、図８に示すフレームが組み立てられた時刻を示す情報が格納される。具体的には、図８のデータフレームを隣接ノード装置に転送する時刻を示す情報が格納される。ボディには、データ本体が格納される。

【０１０１】

署名には、フレーム（正確には平文フレーム）自体のハッシュコードが共通鍵により暗号化された値が格納される。署名により、図８に示すフレームが同一の共通鍵を保有するノード装置において生成されたものであることが証明される。

【０１０２】

図８に示すデータフレームは、通信相手のノード装置のアクセスキー（つまり外部由来アクセスキー）により暗号化されて送信される。

本実施形態に係るノード装置１は、通信相手のノード装置から暗号化フレームを受信すると、自ノード装置が生成したアクセスキーを用いて復号して、平文フレームを得る。ノード装置１はさらに、平文フレームから署名として付与されている暗号化されたハッシュ値を取り出し、さらに、取り出したハッシュ値（暗号化されたハッシュ値）を、共通鍵を用いて復号する。そして、共通鍵を用いて復号して得られた値と、平文フレームから計算されるハッシュ値とを比較し、互いに一致する場合は、ノード装置１は、「自ノード装置と同一の共通鍵を保有するノード装置において生成したフレームが受信された」と判定する。

【０１０３】

また、本実施形態に係るノード装置１は、相手から受信したデータフレームのＦＩＤと時刻情報との組み合わせを記憶しておき、記憶されているＦＩＤ及び時刻情報と受信したデータフレームのＦＩＤ及び時刻情報とを比較する。例えば、正当と認証された２台のノ

ード装置間で通信を行っているときに、不正なノード装置がデータフレームをキャプチャ及びコピーして送信してくることがある。その場合、データフレームに含まれるＦＩＤ及び時刻情報は、過去に正当なノード装置から受信したＦＩＤ及び時刻情報と一致する。このように、受信したデータフレームのＦＩＤ及び時刻情報が、ノード装置１自身が記憶しているＦＩＤ及び時刻情報と一致する場合は、ノード装置１は、不正なノード装置からのアクセスと判断して、受信したデータフレームを破棄する。

【０１０４】

なお、正当なノード装置からデータフレームが再送された場合には、ＦＩＤについては記憶されているＦＩＤと一致するが、時刻情報が異なる。このように、「ＦＩＤは記憶されている値と一致し、時刻情報については異なる」というデータフレームについては、ノード装置１は、既に受信したデータフレームと同一であると判断し、そのデータフレームについても破棄する。

【０１０５】

続いて、上記図６～図８を参照して説明した一連の処理について、図９～図１６のフローチャートを参照しながら、より詳細に説明する。

図９は共通鍵更新処理のフローチャートである。共通鍵更新処理は、ノード装置１の電源が入れられると開始される。

【０１０６】

ステップＳ１０１で、ノード装置１全体を制御する図４のＭＰＵ１１は、図５の時計３３を参照して、現在時刻を認識し、現在時刻が予め決められた更新時刻であるか否かを判断する。なお、ここで「更新時刻」とは、共通鍵の更新を行う時刻として予め決められた時刻である。例えば、t_2＝１２（時間）である場合、「毎日１時と１３時が更新時刻である」と決められていてもよい。

【０１０７】

現在時刻が更新時刻であれば、処理はステップＳ１０２に進み、ＭＰＵ１１は、耐タンパ性ＰＩＣマイコン１４のドライバ（以下「耐タンパデバイスドライバ」という）に、共通鍵の生成のための処理を開始するよう命令する。耐タンパデバイスドライバは、共通鍵生成部３の一部として働く。

【０１０８】

すなわち、ＭＰＵ１１は、共通鍵を生成するための種（seed）として使うデータ（以下「種データ」という）を、耐タンパデバイスドライバに引数として与える。耐タンパデバイスドライバも、ＭＰＵ１１により実行されるプログラムの１種である。

【０１０９】

続いて、ステップＳ１０３において耐タンパデバイスドライバは、受け取った種データを、耐タンパデバイスである耐タンパ性ＰＩＣマイコン１４に出力し、当該種データを使って新たな共通鍵を生成するよう、耐タンパ性ＰＩＣマイコン１４に命令する。

【０１１０】

そして、ステップＳ１０４で耐タンパ性ＰＩＣマイコン１４は、受け取った種データを使って新たな共通鍵を生成し、生成した共通鍵を耐タンパデバイスドライバに通知する。耐タンパデバイスドライバは、生成された新たな共通鍵を、例えばＤＲＡＭ１５上に実現される共通鍵格納部３２に格納する。

【０１１１】

以上のようにして、現在時刻が更新時刻であれば、共通鍵が更新される。他方で、現在時刻が更新時刻でなければ、処理はステップＳ１０１に戻る。なお、ステップＳ１０１の分岐は、タイマ割り込みにより実現されてもよい。

【０１１２】

続いて、アクセスキーの更新について図１０を参照して説明する。図７に関して説明したように、アクセスキーは定期的に更新される。

図１０はアクセスキー更新処理のフローチャートである。

【０１１３】

ステップＳ２０１で、ノード装置１内部のタイマカウンタ（すなわち図４のタイマＩＣ１３により実現される図５のカウンタ３４）がカウントアップ操作を行う。

そして、ステップＳ２０２で、アクセスキー生成部２は、所定の時間t_1＝１０分が経過したか否かを、カウンタ３４の値を参照して判断する。所定の時間t_1＝１０分が経過していれば（すなわち、カウンタ３４の値が、t_1＝１０分に対応する値として予め設定された値に達していれば）、処理はステップＳ２０３に進み、まだ所定の時間t_1＝１０分が経過していなければ、処理はステップＳ２０１に戻る。

【０１１４】

ステップＳ２０３でアクセスキー生成部２は、所定のアルゴリズムにしたがって新たなアクセスキーを生成し、アクセスキー格納部３１に記憶された内部由来アクセスキーを上書き更新する。

【０１１５】

また、ステップＳ２０４では、タイマカウンタ（つまり図５のカウンタ３４）のクリア動作が行われ、その後、処理はステップＳ２０１に戻る。

なお、カウント値が所定の時間t_2に相当する値になるとクリアされる不図示の第２のカウンタ（つまり図５のカウンタ３４とは別のカウンタ）を利用して、図９の共通鍵更新処理を実現することもできる。あるいは逆に、アクセスキー生成部２が時計３３を参照し、現在時刻がアクセスキーの更新時刻に該当するか否かを判断することで、図１０のアクセスキー更新処理を実現することもできる。

【０１１６】

ところで、多数のノード装置１を含むアドホック通信システムにおいては、アドホック通信システム全体としてトラフィックが時間的に分散することが好ましい。アクセスキーの更新に伴うハローフレームの送信は、例えば下記（１）～（３）により、アドホック通信システム内で時間的に分散させることができる。

（１）図２の各ノード装置１Ａ～１Ｉが、共通の所定時間が電源投入後に経過してから図１０の処理を開始するよう設定されている場合は、各ノード装置１Ａ～１Ｉには、時刻をずらして電源が入れられる。すると、各ノード装置１Ａ～１Ｉによるアクセスキーの更新時刻も分散するので、アクセスキーの更新に続いて生じるハローフレームの送信も、時間的に分散して生じることになる。

【０１１７】

（２）各ノード装置１Ａ～１Ｉは、ノード装置１Ａ～１Ｉごとに異なるランダムな時間が電源投入後に経過してから図１０の処理を開始するように設定されていてもよい。例えば、各ノード装置１Ａ～１Ｉそれぞれのフラッシュメモリ１６の所定の領域に、上記ランダムな時間が予め書き込まれて設定されてもよい。

【０１１８】

（３）各ノード装置１Ａ～１Ｉにおいて、上記の所定の時間t_1の長さが異なるよう、設定されていてもよい。所定の時間t_1は、例えば、ＭＰＵ１１が実行するファームウェアプログラムで利用される定数として、予め設定されている。

【０１１９】

さて、上記のようにして図１０の処理によりアクセスキーが生成されると、図７のステップＳ１とＳ２に関して説明したように、ハローフレームが送信される。生成された新たなアクセスキーは、ハローフレームにより、隣接するノード装置に通知される。

【０１２０】

そこで、以下ではハローフレームの送信と受信の詳細について、図１１～図１３を参照して説明する。

図１１はハローフレーム送信処理のフローチャートである。また、図１２はハローフレームのフォーマットと、ハローフレームに関して行われる各種処理を説明する図である。

【０１２１】

図１１の処理は、アクセスキー生成部２がアクセスキーを生成したことを契機として開始される。例えば、図７のステップＳ１ではノード装置１Ａが、ステップＳ２ではノード

装置１Ｂが、図１１の処理を実行する。例えば、アクセスキー生成部２がアクセスキーの生成をハローフレーム作成部３６に通知することで、ハローフレーム作成部３６が図１１の処理を開始する。

【０１２２】

ステップＳ３０１においてハローフレーム作成部３６は、ハローデータ（すなわちハローフレームのペイロードの元になる平文データ）と、ハローフレームのヘッダを作成する。具体的には、ハローデータは、アクセスキー生成部２が新たに生成したアクセスキーのデータを含む。

【０１２３】

例えば、ハローフレームはアクセスキーの交換のために予め決められた所定のフォーマットのフレームであればよく、ペイロードにはアクセスキー以外の様々なフィールドを含んでもよい。しかし、以下では説明の簡単化のため、本実施形態のハローフレームは、ペイロードに暗号化されたアクセスキーのみを含む場合を例として説明する。

【０１２４】

この場合、ステップＳ３０１でハローフレーム作成部３６は、単にアクセスキー格納部３１からハローデータとして内部由来アクセスキーを読み出すだけで、ハローデータを用意することができる。すなわち、図１２の平文アクセスキーＤ１が、ステップＳ３０１でハローデータとして用意される。

【０１２５】

次に、ステップＳ３０２においてハローフレーム作成部３６は、ハローデータのハッシュ値を計算し、計算したハッシュ値を、ハローフレームの元になる平文フレームの末尾に署名として付与する。具体的には、ハローフレーム作成部３６は、図１２の平文アクセスキーＤ１から平文ハッシュ値Ｄ２を計算し、ヘッダと平文アクセスキーＤ１と平文ハッシュ値Ｄ２を連結した平文フレームを、ハローフレーム暗号化部３７に出力する。なお、「平文ハッシュ値」という名称は、暗号化されたハッシュ値と対比して、暗号化される前の元のハッシュ値であることを明示するための名称である。

【０１２６】

そして、ステップＳ３０３でハローフレーム暗号化部３７は、共通鍵格納部３２を参照して共通鍵を読み出し、ステップＳ３０２で署名が付与された後の平文フレーム（正確には、平文フレームのペイロードとトレイラ）を、共通鍵を用いて暗号化する。

【０１２７】

例えば、本実施形態では、暗号化アルゴリズムとして、ストリーム暗号の１種であるＲＣ４が採用されている。よって、ステップＳ３０３では、ハローフレーム暗号化部３７が共通鍵から鍵ストリームを生成し、平文アクセスキーＤ１と平文ハッシュ値Ｄ２からなる部分と、鍵ストリームとの排他的論理和（ＸＯＲ；eXclusive OR）を求める。それにより、ステップＳ３０３では、暗号化されたペイロード及びトレイラが生成される。

【０１２８】

具体的には、図１２に示すように、ハローフレーム暗号化部３７は、平文アクセスキーＤ１から暗号化アクセスキーＤ３を生成し、平文ハッシュ値Ｄ２から暗号化ハッシュ値Ｄ４を生成する。なお、図１２では、共通鍵を使った暗号化又は復号化の操作を黒い太矢印で表している。

【０１２９】

また、ステップＳ３０１で用意されたヘッダは暗号化されず、クリアテキスト（cleartext）のまま使われる。本実施形態では、例えば図１２に示すように、ローカル宛先アドレスＤ５、ローカル差出アドレスＤ６、フレームタイプＤ７及びフレームサイズＤ８の各フィールドを含むアドホックヘッダＤ９がステップＳ３０１で用意されている。

【０１３０】

したがって、ステップＳ３０３でハローフレーム暗号化部３７は、アドホックヘッダＤ９に、ペイロードＤ１０としての暗号化アクセスキーＤ３と、トレイラＤ１１としての暗号化ハッシュ値Ｄ４とを連結し、ハローフレームを作成する。そして、ハローフレーム暗

号化部３７は、作成したハローフレームをハローフレーム送信バッファ４１に出力する。
【０１３１】
なお、本実施形態では、隣接する複数の装置（他のノード装置やゲートウェイ装置ＧＷ）にアクセスキーを通知するため、ハローフレームはブロードキャストされる。そのため、具体的には、ローカル宛先アドレスＤ５はブロードキャストアドレスであり、ローカル差出アドレスＤ６はノード装置１自身のＭＡＣアドレスである。
【０１３２】
また、フレームタイプＤ７は、ハローフレームを表す値に設定されている。フレームサイズＤ８には、暗号化アクセスキーＤ３と暗号化ハッシュ値Ｄ４の長さの和（すなわち平文アクセスキーＤ１と平文ハッシュ値Ｄ２の長さの和）が指定されている。
【０１３３】
最後に、ステップＳ３０４で送信部７はハローフレームを送信する。すなわち、ステップＳ３０３の結果として一時的にハローフレーム送信バッファ４１に格納されたハローフレームが、送信処理部４４によってステップＳ３０４で読み出されて送信される。
【０１３４】
図１３はハローフレーム受信処理のフローチャートである。例えば、図７のステップＳ１においては、図２のノード装置１Ａが図１１の処理を行うので、ノード装置１Ａに隣接するノード装置１Ｂで図１３の処理が行われる。
【０１３５】
ノード装置１Ｂにおいて、受信部８がハローフレームを受信すると、フレーム分岐処理部２１が「受信したフレームはハローフレームである」とアドホックヘッダＤ９のフレームタイプＤ７から判別する。そして、その判別を契機として、図１３の処理が開始される。また、フレーム分岐処理部２１によってハローフレームと判別された受信フレームは、一時的にハローフレーム受信バッファ２２に格納される。
【０１３６】
ステップＳ４０１で復号化部５のハローフレーム復号化部２５は、共通鍵格納部３２を参照して共通鍵のデータを読み出す。そして、ハローフレーム復号化部２５は、共通鍵を用いて、ハローフレーム受信バッファ２２に格納されているハローフレーム（本実施形態では、正確にはそのペイロードとトレイラ）を復号する。
【０１３７】
すなわち、ハローフレーム復号化部２５は、共通鍵から鍵ストリームを生成し、ペイロードＤ１０とトレイラＤ１１からなる部分と鍵ストリームとのＸＯＲを求める。それにより、ハローフレーム復号化部２５は、暗号化アクセスキーＤ３から、復号された平文アクセスキーＤ１２を得るとともに、暗号化ハッシュ値Ｄ４から、復号された平文ハッシュ値Ｄ１３を得る。そして、ハローフレーム復号化部２５は、アドホックヘッダＤ９と復号された平文アクセスキーＤ１２と復号された平文ハッシュ値Ｄ１３からなる平文フレームを確認部２９に出力する。
【０１３８】
すると、ステップＳ４０２で確認部２９は、ハローフレーム復号化部２５から入力された平文フレームから、復号された平文アクセスキーＤ１２を抽出する。そして、確認部２９は、復号された平文アクセスキーＤ１２のハッシュ値を計算し、図１２の計算されたハッシュ値Ｄ１４を得る。
【０１３９】
そして、ステップＳ４０３で確認部２９は、図１２の復号された平文ハッシュ値Ｄ１３と計算されたハッシュ値Ｄ１４を比較する。
２つのハッシュ値が等しければ、確認部２９は「ＯＫ」と判断し、処理はステップＳ４０４に移行する。他方、２つのハッシュ値が異なれば、確認部２９は「ＮＧ」と判断し、処理はステップＳ４０５に移行する。
【０１４０】
ステップＳ４０４では、確認部２９が、ローカル差出アドレスＤ６と関連付けられてい

るアクセスキー格納部２８内の外部由来アクセスキーを、復号された平文アクセスキーＤ１２で上書きする。その結果、ハローフレームの送信元のノード装置に対応する外部由来アクセスキーが更新される。そして図１３の処理は終了する。

【０１４１】

他方、ステップＳ４０５では、図１３の処理を開始する契機となった当該ハローフレームが廃棄され、図１３の処理が終了する。

以上、図７のステップＳ１とＳ２に対応する処理の詳細を、図１０～図１３を参照して説明したので、続いて、図７のステップＳ３とＳ４に対応する処理の詳細を、図１４～図１６を参照して説明する。

【０１４２】

図１４はデータフレーム送信処理のフローチャートである。図7のステップＳ３ではノード装置１Ａが、ステップＳ４ではノード装置１Ｂが、図１４の処理を行う。実施形態に応じて、例えば、ノード装置１に接続されたセンサ等の外部機器からの入力を契機としてデータフレーム送信処理が開始されてもよい。あるいは、ノード装置１は、予め決められたスケジュールにしたがってデータフレーム送信処理を行ってもよい。

【０１４３】

本実施形態では、下記（１）～（３）の条件が成立すると、データフレーム作成部４０が図１４の処理を開始する。

（１）送信対象のデータ（以下「対象データ」という）が用意される。対象データは、例えば、ノード装置１に接続された外部機器から入力されてもよいし、データフレーム作成部４０が作成してもよい。対象データの例は、図２に関して説明したセンサデータである。

【０１４４】

（２）最終的な宛先（すなわちアドホックネットワーク内でのグローバルな宛先）が決定される。最終的な宛先は、図２の例のように固定的にゲートウェイ装置ＧＷと決定されていてもよいし、データフレーム作成部４０により動的に決定されてもよい。

【０１４５】

（３）グローバルな宛先から、ローカルな宛先（すなわち隣接する他のノード装置のうちの１つ）が決定される。アドホック通信システムの構成要素であるノード装置１は、グローバルな宛先からローカルな宛先を決定することができる。

【０１４６】

なお、上記（３）に関して補足すると次のとおりである。

図１に関して説明したように、アドホック通信システムの構成要素であるノード装置１は、ノード装置１自身の周囲に存在する他のノード装置についてリストを作成し、リストに基づいてノード装置１がフレームを転送するノード装置を決定することができる。つまり、ノード装置１には、グローバルな宛先からローカルな宛先を決定してフレームをルーティングする機能が実装されている。

【０１４７】

例えば、図２のノード装置１Ｂは、ノード装置１Ｂ自身の周囲に存在する他のノード装置１Ａ、１Ｃ及び１Ｅについてリストを作成し、「最終的な宛先がゲートウェイ装置ＧＷのフレームは、ノード装置１Ｃに転送するのが好ましい」といった情報を管理する。つまり、ノード装置１Ｂは、グローバルな宛先（例えばゲートウェイ装置ＧＷ）を、ノード装置１Ｂ自身に隣接する装置を示すローカルな宛先（例えばノード装置１Ｃ）に対応付けて管理し、フレームのルーティングを行う。グローバルな宛先とローカルな宛先を対応付ける情報は、例えば図４のＤＲＡＭ１５に記憶される。

【０１４８】

また、グローバルな宛先とローカルな宛先を対応付ける情報は、重み付けされていてもよい。重み付けにより、ある１つのグローバルな宛先（例えばゲートウェイ装置ＧＷ）に関して、ノード装置１Ｂ自身に隣接する複数の装置（例えばノード装置１Ａ、１Ｃ及び１Ｅ）のうち、いずれが転送先として好ましいかが表される。例えば、図２の例では、ゲー

トウェイ装置ＧＷとノード装置１Ａの組の重みよりも、ゲートウェイ装置ＧＷとノード装置１Ｃの組の重みの方が、高い優先度を示す。すなわち、重み付けにより、「最終的な宛先がゲートウェイ装置ＧＷのフレームは、ノード装置１Ａ又は１Ｅに転送するよりも、ノード装置１Ｃに転送する方が好ましい」といった情報が表される。

【０１４９】

ＭＰＵ１１は、ファームウェアプログラムを実行することにより、上記の情報を管理し、受信したフレームの転送の要否を判断する。転送が必要な場合、ファームウェアプログラムを実行するＭＰＵ１１は、ＤＲＡＭ１５を参照してグローバルな宛先からローカルな宛先を決定し、決定したローカルな宛先を転送先として、フレームを送信する。

【０１５０】

ここで図１４の説明に戻ると、上述のとおりデータフレーム送信処理は、上記（１）～（３）の条件が成立すると開始される。

すると、ステップＳ５０１でデータフレーム作成部４０は、データフレームのペイロードの元になる平文ペイロードのハッシュ値を計算する。データフレーム作成部４０は、計算したハッシュ値を、平文ペイロードの末尾に続く平文トレイラの一部として付与する。本実施形態は、トレイラには、署名が設定される。

【０１５１】

ここで、図１５を参照してステップＳ５０１をより詳細に説明すれば下記のとおりである。

図１５はデータフレームのフォーマットと、データフレームに関して行われる各種処理の第１の例を説明する図である。図１５は、図８と一部異なるフォーマットが採用される場合についての説明である。図８と同様のフォーマットを採用する場合については、図１７とともに後述する。

【０１５２】

ステップＳ５０１でデータフレーム作成部４０は、図１５の平文ＦＩＤ・Ｄ１５として新たなＦＩＤを発行する。また、データフレーム作成部４０は、上記の条件（１）に関して説明した対象データだけでなく、ペイロードに含める他のデータを適宜ステップＳ５０１で用意する。ステップＳ５０１で用意されるデータは、ＤＲＡＭ１５又はフラッシュメモリ１６から読み出されるデータでもよいし、データフレーム作成部４０によって生成されるデータでもよいし、外部機器から入力されるデータでもよい。

【０１５３】

例えば、データフレーム作成部４０は、データフレームの最終的な宛先であるグローバルな宛先を指定するデータを、条件（１）で用意された対象データと合わせて、平文ボディＤ１６を作成する。

【０１５４】

また、図１４には明示していないが、データフレーム作成部４０はステップＳ５０１でさらに、アドホックヘッダＤ９を生成する。アドホックヘッダＤ９の形式は、ハローフレームと同様である。

【０１５５】

すなわち、データフレームにおいても、アドホックヘッダＤ９は、ローカル宛先アドレスＤ５、ローカル差出アドレスＤ６、フレームタイプＤ７及びフレームサイズＤ８を含む。ただし、ローカル宛先アドレスＤ５は上記の条件（３）で説明したようにして決定されたＭＡＣアドレスである。また、フレームタイプＤ７は、データフレームを示す値に設定される。

【０１５６】

こうして、データフレーム作成部４０はステップＳ５０１においてアドホックヘッダＤ９と、平文ＦＩＤ・Ｄ１５と平文ボディＤ１６からなる平文ペイロードとを作成し、平文ペイロードから図１５の平文ハッシュ値Ｄ１７を計算する。

【０１５７】

また、ステップＳ５０２でデータフレーム作成部４０は、時計３３を参照して現在時刻

情報を取得し、取得した現在時刻情報を図１５の平文時刻Ｄ１８として、平文ハッシュ値Ｄ１７の後ろに連結する。平文ハッシュ値Ｄ１７と平文時刻Ｄ１８からなる部分が、暗号化署名の元となる平文署名である。そして、データフレーム作成部４０は、アドホックヘッダＤ９、平文ペイロード及び平文署名からなる平文フレームをデータフレーム暗号化部３９に出力する。

【０１５８】

すると、ステップＳ５０３でデータフレーム暗号化部３９は、共通鍵格納部３２を参照して共通鍵を読み出し、共通鍵を用いて平文署名を暗号化して暗号化署名Ｄ２１を得る。

上記のように、本実施形態では暗号化アルゴリズムとしてＲＣ４が採用されている。よって、ステップＳ５０３でデータフレーム暗号化部３９は、具体的には、共通鍵から鍵ストリームを生成し、平文署名と鍵ストリームとのＸＯＲを求める。

【０１５９】

その結果、平文ハッシュ値Ｄ１７からは暗号化ハッシュ値Ｄ１９が得られ、平文時刻Ｄ１８からは暗号化時刻Ｄ２０が得られる。換言すれば、平文署名全体からは、暗号化ハッシュ値Ｄ１９と暗号化時刻Ｄ２０からなる暗号化署名Ｄ２１が得られる。

【０１６０】

続いて、ステップＳ５０４でデータフレーム暗号化部３９は、上記条件（３）で決定した送信先のノード装置（すなわち、ローカル宛先アドレスＤ５にＭＡＣアドレスが指定されているノード装置）のアクセスキーを使って、平文フレームを暗号化する。すなわち、データフレーム暗号化部３９は、アクセスキー格納部２８を参照して送信先のノード装置のアクセスキーを読み出し、読み出したアクセスキーを用いて、平文ペイロードと暗号化署名Ｄ２１を暗号化する。

【０１６１】

すなわち、データフレーム暗号化部３９は、鍵ストリームの生成とＸＯＲ演算を行う。その結果、データフレーム暗号化部３９は、平文ＦＩＤ・Ｄ１５からは暗号化ＦＩＤ・Ｄ２２を、平文ボディＤ１６からは暗号化ボディＤ２３を、それぞれ生成する。また、データフレーム暗号化部３９は、暗号化ハッシュ値Ｄ１９からは二重暗号化ハッシュ値Ｄ２４を、暗号化時刻Ｄ２０からは二重暗号化時刻Ｄ２５を生成する。つまり、暗号化署名Ｄ２１からは、トレイラに相当する、二重に暗号化された署名が得られる。

【０１６２】

なお、図１５及び図１７では、共通鍵による暗号化及び復号化を黒い矢印で表し、アクセスキーによる暗号化及び復号化を斜線模様の矢印で表している。

以上のようにして、暗号化ＦＩＤ・Ｄ２２と暗号化ボディＤ２３からなるペイロードＤ２６と、二重暗号化ハッシュ値Ｄ２４と二重暗号化時刻Ｄ２５からなる署名としてのトレイラＤ２７が生成される。したがって、ステップＳ５０４でデータフレーム暗号化部３９は、アドホックヘッダＤ９にペイロードＤ２６とトレイラＤ２７を連結してデータフレームを作成し、データフレーム送信バッファ４３に出力する。

【０１６３】

最後に、ステップＳ５０５で送信部７はデータフレームを送信する。すなわち、ステップＳ５０４の結果として一時的にデータフレーム送信バッファ４３に格納されたデータフレームが、送信処理部４４によってステップＳ５０５で読み出されて送信される。

【０１６４】

図１６はデータフレーム受信処理のフローチャートである。図７のステップＳ３では１Ｂが、ステップＳ４ではノード装置１Ａが、図１６の処理を行う。

以下、説明の便宜上、図７のステップＳ３で、ノード装置１Ｂが、アクセスキーｂ１で暗号化されたデータフレームを受信部８において受信した場合について、説明する。

【０１６５】

上記データフレームがノード装置１Ｂで受信されると、フレーム分岐処理部２１は、「受信したフレームはデータフレームである」とアドホックヘッダＤ９のフレームタイプＤ７から判別する。そして、その判別を契機として、図１６の処理が開始される。また、フ

レーム分岐処理部２１によってデータフレームと判別された受信フレームは、一時的にデータフレーム受信バッファ２４に格納される。

【０１６６】

ステップＳ６０１で復号化部５のデータフレーム復号化部２７は、自ノード装置１Ｂのアクセスキーを使って、受信したフレームを復号する。すなわち、データフレーム復号化部２７は、アクセスキー格納部３１を参照して、ノード装置１Ｂ自身にとっては内部由来アクセスキーであるアクセスキーｂ１のデータを読み出す。そして、データフレーム復号化部２７は、アクセスキーｂ１を用いて、データフレーム受信バッファ２４に格納されているデータフレーム（本実施形態では、正確にはそのペイロードとトレイラ）を復号する。

【０１６７】

すなわち、データフレーム復号部２７は、アクセスキーｂ１から鍵ストリームを生成し、暗号文（つまり図１５のペイロードＤ２６とトレイラＤ２７からなる部分）と鍵ストリームとのＸＯＲを求める。それにより、データフレーム復号部２７は、暗号化ＦＩＤ・Ｄ２２から、復号された平文ＦＩＤ・Ｄ２８を得、暗号化ボディＤ２３から、復号された平文ボディＤ２９を得る。また、データフレーム復号部２７は、二重暗号化ハッシュ値Ｄ２４から、復号された暗号文ハッシュ値Ｄ３０を得、二重暗号化時刻Ｄ２５から、復号された暗号文時刻Ｄ３１を得る。つまり、データフレーム復号部２７は二重暗号化署名から暗号化署名を得る。

【０１６８】

続いて、ステップＳ６０２でデータフレーム復号部２７は、共通鍵格納部３２を参照して共通鍵のデータを読み出し、復号された暗号文ハッシュ値Ｄ３０と復号された暗号文時刻Ｄ３１からなる暗号化署名を、共通鍵を用いて復号する。その結果、復号された暗号文ハッシュ値Ｄ３０からは復号された平文ハッシュ値Ｄ３３が得られ、復号された暗号文時刻Ｄ３１からは復号された平文時刻Ｄ３４が得られる。

【０１６９】

そこで、データフレーム復号部２７は、アドホックヘッダＤ９、復号された平文ＦＩＤ・Ｄ２８、復号された平文ボディＤ２９、復号された平文ハッシュ値Ｄ３３及び復号された平文時刻Ｄ３４を、復号された平文フレームとして確認部２９に出力する。

【０１７０】

ステップＳ６０３で確認部２９は、データフレーム復号部２７からの入力から、復号された平文ＦＩＤ・Ｄ２８と復号された平文ボディＤ２９からなる部分（以下、「復号された平文ペイロード」という）を抽出する。そして、確認部２９は、復号された平文ペイロードのハッシュ値を計算し、図１５の計算されたハッシュ値Ｄ３２を得る。

【０１７１】

ステップＳ６０３では、受信されたデータフレームの認証判定処理として、確認部２９が、計算されたハッシュ値Ｄ３２と復号された平文ハッシュ値Ｄ３３を比較する。受信されたデータフレームが、改竄などを受けていない正しいデータフレームであれば、計算されたハッシュ値Ｄ３２と復号された平文ハッシュ値Ｄ３３は一致する。

【０１７２】

よって、計算されたハッシュ値Ｄ３２と復号された平文ハッシュ値Ｄ３３が一致する場合、確認部２９は「ＯＫ」と判定して、処理はステップＳ６０４に移行する。他方、計算されたハッシュ値Ｄ３２と復号された平文ハッシュ値Ｄ３３が一致しない場合は、確認部２９は「ＮＧ」と判定して、処理はステップＳ６０８に移行する。

【０１７３】

ステップＳ６０４で確認部２９は、復号された平文時刻Ｄ３４を抽出する。ステップＳ６０４が実行されるのはステップＳ６０３で「ＯＫ」と判断された場合なので、復号された平文時刻Ｄ３４は、元の平文時刻Ｄ１８と等しい。また、確認部２９は、ステップＳ６０４でローカル差出アドレスＤ６も抽出する。

【０１７４】

そして、ステップＳ６０５で確認部２９は、時刻判定処理を行う。時刻判定処理は、なりすまし攻撃に対する防御のための処理である。なお、本明細書では、不正な第三者がデータフレームを傍受（すなわちキャプチャ）し、傍受したデータフレームをコピー又は一部変更して送信することを、なりすまし攻撃という。

【０１７５】

具体的には、確認部２９は、図５の最新送信時刻格納部４５を参照して時刻判定処理を行う。図１６に示すように、最新送信時刻格納部４５は、ローカル差出アドレスと時刻を対応付けるエントリを記憶する。

【０１７６】

例えば、図１６に示した１番目のエントリは、ローカル差出アドレスA_1と時刻T_1とを対応付けている。また、上記のように、図１６の説明は、ノード装置１Ｂが図１６の処理を行う場合を例としている。したがって、図１６に示す１番目のエントリは、「ローカル差出アドレスA_1で識別されるノード装置からノード装置１Ｂが受信した最新のデータフレームから得られた、復号された平文時刻Ｄ３４は、T_1である」ということを示す。

【０１７７】

ノード装置１Ｂの電源が投入された時点、すなわち初期状態での最新送信時刻格納部４５は、１つもエントリを記憶していないが、後述のステップＳ６０６により、最新送信時刻格納部４５にエントリが追加され、又は既存のエントリが更新される。

【０１７８】

ステップＳ６０５において、確認部２９は、抽出したローカル差出アドレスＤ６を検索キーにして最新送信時刻格納部４５を検索する。検索の結果、「ローカル差出アドレス」フィールドが、抽出したローカル差出アドレスＤ６と一致するエントリがなければ、確認部２９は、「受信したデータフレームは、なりすまし攻撃によって送られたデータフレームではない」と判断する。すなわち、確認部２９は、「受信したデータフレームは、正当なデータフレームである」と判断し、処理はステップＳ６０６に移行する。

【０１７９】

逆に、検索の結果、「ローカル差出アドレス」フィールドが、抽出したローカル差出アドレスＤ６と一致するエントリが見つかった場合、受信したデータフレームは、なりすまし攻撃によって送られた可能性がある。そこで、確認部２９は、見つかったエントリの「時刻」フィールドの値を、ステップＳ６０４で抽出した、復号された平文時刻Ｄ３４と比較する。

【０１８０】

２つの時刻が一致する場合、確認部２９は、「受信したデータフレームがなりすまし攻撃によるものである」と判断し、処理はステップＳ６０８に移行する。逆に、２つの時刻が一致しなければ、確認部２９は、「ローカル差出アドレスＤ６で識別されるノード装置から、今までにノード装置１Ｂが受信したのとは異なる新たなデータフレームが、正当に送信された」と判断し、処理はステップＳ６０６に移行する。

【０１８１】

ステップＳ６０６で確認部２９は、ローカル差出アドレスＤ６で識別される送信元ノード装置の最新時刻情報を更新する。

すなわち、ステップＳ６０５の検索でエントリが見つからなかった場合には、確認部２９は、ローカル差出アドレスＤ６と復号された平文時刻Ｄ３４を対応付ける新たなエントリを作成して最新送信時刻格納部４５に格納する。また、ステップＳ６０５の検索でエントリが見つかった場合には、確認部２９は、見つかった当該エントリの「時刻」フィールドの値を、復号された平文時刻Ｄ３４で上書きする。

【０１８２】

以上により最新送信時刻格納部４５が保持する最新時刻情報を更新すると、確認部２９は、平文フレームを受信データフレーム処理部３０に出力する。

すると、ステップＳ６０７では、受信データフレーム処理部３０が、確認部２９からの入力を用いて、実施形態に応じた処理を行う。

【０１８３】
例えば、復号された平文ボディＤ２９には、対象データの最終的な宛先（つまりグローバルな宛先）が指定されていてもよい。そして、受信データフレーム処理部３０は、グローバルな宛先に応じて、データフレームの転送の要否を判断し、転送する場合にはローカルな宛先を決定し、新たなデータフレームの組み立てをデータフレーム作成部４０に命令してもよい。
【０１８４】
また、受信データフレーム処理部３０は、図８に関して説明したように、復号された平文ＦＩＤ・Ｄ２８と復号された平文時刻Ｄ３４を用いて、不正なデータフレームと正当なデータフレームの判別や、受信したデータフレームが再送されたものか否かの判断を行ってもよい。
【０１８５】
また、ステップＳ６０８では、受信されたデータフレームが廃棄され、図１６の処理が終了する。すなわち、ステップＳ６０８では、確認部２９は、受信データフレーム処理部３０にデータを出力しない。
【０１８６】
以上図１４～図１６を参照して説明したデータフレームの送受信に関する一連の処理は、データフレームのフォーマットに応じて適宜変形可能である。その具体例を、図１７とともに説明する。
【０１８７】
図１７は、データフレームのフォーマットと、データフレームに関して行われる各種処理の第２の例を説明する図である。図１７は図８を詳細化したフォーマットの一例である。
【０１８８】
以下、ノード装置１Ａからノード装置１Ｂへデータフレームが送信される場合を例にして、図１７に対応する処理の詳細を説明する。
ノード装置１Ａのデータフレーム作成部４０は、平文ＦＩＤ・Ｄ１５と平文時刻Ｄ１８と平文ボディＤ１６からなる平文ペイロードのハッシュ値を計算し、平文ハッシュ値Ｄ３５を得る。そして、ノード装置１Ａのデータフレーム暗号化部３９は、共通鍵を使って平文ハッシュ値Ｄ３５を暗号化して暗号化ハッシュ値Ｄ３６を得、平文ペイロードと暗号化ハッシュ値Ｄ３６からなる部分を、ノード装置１Ｂのアクセスキーｂ１で暗号化する。
【０１８９】
その結果、平文ＦＩＤ・Ｄ１５からは暗号化ＦＩＤ・Ｄ３７が、平文時刻Ｄ１８からは暗号化時刻Ｄ３８が、平文ボディＤ１６からは暗号化ボディＤ３９が、暗号化ハッシュ値Ｄ３６からは二重暗号化ハッシュ値Ｄ４０が得られる。
【０１９０】
ノード装置１Ａのデータフレーム暗号化部３９は、アドホックヘッダＤ９に、暗号化ＦＩＤ・Ｄ３７と暗号化時刻Ｄ３８と暗号化ボディＤ３９からなるペイロードＤ４１と、トレイラＤ４２としての二重暗号化ハッシュ値Ｄ４０を連結する。連結により完成した、暗号化されたデータフレームは、データフレーム送信バッファ４３に一時的に格納され、送信処理部４４から送信される。
【０１９１】
そして、暗号化されたデータフレームを受信したノード装置１Ｂでは、フレーム分岐処理部２１がフレームタイプＤ７から「受信したフレームはデータフレームである」と判別し、受信されたフレームはデータフレーム受信バッファ２４に格納される。そして、データフレーム復号部２７がペイロードＤ４１とトレイラＤ４２をノード装置１Ｂ自身のアクセスキーｂ１で復号する。
【０１９２】
その結果、暗号化ＦＩＤ・Ｄ３７からは、復号された平文ＦＩＤ・Ｄ４３が得られ、暗号化時刻Ｄ３８からは、復号された平文時刻Ｄ４４が得られ、暗号化ボディＤ３９からは

、復号された平文ボディＤ４５が得られる。また、二重暗号化ハッシュ値Ｄ４０からは復号された暗号文ハッシュ値Ｄ４６が得られる。データフレーム復号部２７はさらに、復号された暗号文ハッシュ値Ｄ４６を共通鍵で復号することで、復号された平文ハッシュ値Ｄ４８を得る。

【０１９３】

すると、ノード装置１Ｂの確認部２９は、復号された平文ＦＩＤ・Ｄ４３と復号された平文時刻Ｄ４４と復号された平文ボディＤ４５からなる部分のハッシュ値を計算し、計算されたハッシュ値Ｄ４７を得る。そして、確認部２９は、計算されたハッシュ値Ｄ４７と復号された平文ハッシュ値Ｄ４８を比較し、両者が不一致であれば、データフレームを廃棄する。

【０１９４】

計算されたハッシュ値Ｄ４７と復号された平文ハッシュ値Ｄ４８が一致するとき、確認部２９はさらに、ローカル差出アドレスＤ６を検索キーにして最新送信時刻格納部４５を検索し、図１６のステップＳ６０５と同様の時刻判定処理を行う。ステップＳ６０５以降の処理は、図１６に関して説明したのと同様である。

【０１９５】

以上説明したように、本実施形態に係るノード装置は、所定の期間で更新される共通鍵を用いてアクセスキーを交換して、共通鍵及びアクセスキーを利用して第三者による不正なアクセスと正当なノード装置からのアクセスとを判別している。このため、共通鍵やアクセスキーを更新するタイミングをノード装置間で一致させる必要がある。すなわち、ノード装置内の時刻について、ネットワーク内のノード装置間で同期をとっておく必要がある。以下、時刻の同期方法について説明する。

【０１９６】

図１８は、時刻の同期方法を説明する図である。図１８のノード装置１Ａにおいて時刻の同期をとって時刻合わせする場合を例に説明することとする。

ノード装置１Ａは、自ノード装置１Ａの現在時刻と、時刻合わせを行った最終時刻とを記憶部（例えばＤＲＡＭ１５）に記憶させておく。そして、時刻同期用の時刻同期フレームを受信した場合には、時刻同期フレームから時刻に関わる情報を取り出して、自ノード装置１Ａにおいて記憶している情報と比較する。比較した結果、同期が必要と判断した場合には、ノード装置１Ａは、時刻同期フレームに含まれる情報にしたがって時刻合わせを行う。

【０１９７】

時刻同期フレームは、本実施形態においては、ハローフレームと類似のフォーマットの制御用フレームの１種であり、現在時刻及び時刻合わせを行った時刻（以下、「同期時刻」とする）を示すデータを含む。ここで、現在時刻とは、時刻同期フレームを生成する時点でのそのノード装置１自身における時刻を言い、同期時刻とは、所定の装置において時刻の同期をとった時刻を言う。所定の装置とは、本実施形態においてはゲートウェイ装置ＧＷであり、時刻の同期は、例えばＳＮＴＰ（Simple Network Time Protocol）等によりゲートウェイ装置ＧＷにおいて時刻の同期をとることを言う。

【０１９８】

ゲートウェイ装置ＧＷにおいて、定期的に、例えば２時間に１回、ＳＮＴＰ等により時刻の同期をとる。各ノード装置１は、時刻同期フレームに、自ノード装置１の現在時刻と同期時刻とを格納し、時刻同期フレームによりブロードキャストする。時刻同期フレームは、所定のタイミングで（例えば２時間に１回）、上記の時間変化する共通鍵とは異なる固定的な時刻同期鍵を用いて暗号化して送信される。

【０１９９】

図１８に示す例では、ゲートウェイ装置ＧＷにおいて、１２時にＳＮＴＰ等により時刻の同期をとり、１３時に時刻同期フレームＰ１を生成して送信する。

時刻同期フレームＰ１を受信したノード装置１Ａは、自ノード装置１Ａに記憶している最終同期時刻と、時刻同期フレームＰ１の同期時刻とを比較する。図１８の例では、時刻

同期フレームＰ１の同期時刻（１２：００）の方が記憶している最終同期時刻（１１：００）よりも新しい。この場合は、ノード装置１Ａは、受信した時刻同期フレームに格納されている現在時刻（１３：００）を現在時刻として設定する。

【０２００】

ここで、ノード装置１Ａは、ノード装置１Ｂから送信される時刻同期フレームＰ２のように、最新でない時刻における同期による時刻同期フレームを受信することがある。時刻同期フレームＰ２を受信した場合は、ノード装置１Ａは、自ノード装置１Ａに記憶している最終同期時刻（１１：００）の方が時刻同期フレームＰ２の同期時刻（１０：００）よりも新しいため、時刻の同期はとらない。

【０２０１】

続いて、図１８の例について、図１９～図２１を参照してより詳細に説明する。

図１９は、図１８を参照して説明した時刻の同期方法を説明するシーケンス図である。図１９には、ＳＮＴＰサーバＳＳ、ゲートウェイ装置ＧＷ及びノード装置１Ａ～１Ｃが示されている。以下では、アドホックネットワーク内でゲートウェイ装置ＧＷとノード装置１Ａが隣接しており、ノード装置１Ａはノード装置１Ｂ及び１Ｃとも隣接しているものとする。

【０２０２】

なお、ゲートウェイ装置ＧＷとノード装置１Ａ～１Ｃは、いずれも図５の各部を備えている。また、ゲートウェイ装置ＧＷにはさらに、ＳＮＴＰによる時刻合わせ機能も実装されている。

【０２０３】

ステップＳ７０１に示すように、ゲートウェイ装置ＧＷは、ゲートウェイ装置ＧＷ自身の時計３３における時刻が１２：００になると、予め決められたスケジュールにしたがって、ＳＮＴＰによってＳＮＴＰサーバＳＳにアクセスし、時刻合わせを行う。

【０２０４】

また、ゲートウェイ装置ＧＷには、時刻同期フレームを送信するタイミングについても、予め「１３：００に送信する」のようなスケジュールが設定されている。よって、ステップＳ７０１での時刻合わせの結果適宜修正されたゲートウェイ装置ＧＷの時計が１３：００を示すと、ゲートウェイ装置ＧＷはステップＳ７０２に示すように、時刻同期フレームＰ１を送信する。

【０２０５】

なお、時刻同期フレームを送信するタイミングは、隣接する複数のノード装置それぞれに対して別の時刻が設定されていてもよい。

時刻同期フレームのフォーマットの詳細の図示は省略するが、時刻同期フレームは、図１２のハローフレームと同様のアドホックヘッダＤ９を含み、さらに、「同期時刻」と「現在時刻」という２つのフィールドを含む平文ペイロードを、時刻同期鍵を使って暗号化して得られる暗号化ペイロードを含む。

【０２０６】

例えば、ステップＳ７０２では、ゲートウェイ装置ＧＷが、「同期時刻が１２：００で現在時刻が１３：００である」と示す時刻同期フレームＰ１を送信する。すなわち、同期時刻フィールドの値は、ゲートウェイ装置ＧＷ自身がステップＳ７０１の時刻合わせを行った時刻であり、現在時刻フィールドの値は、ゲートウェイ装置ＧＷが時刻同期フレームＰ１を送信する時刻である。

【０２０７】

なお、以下では、時刻同期フレームＰ１のローカル宛先アドレスはノード装置１Ａのアドレスであるとする。時刻同期フレーム送信処理の詳細は、図２０とともに後述する。

ところで、本実施形態では、アドホックネットワーク内で互いに隣接する装置間での通信遅延時間は、ゼロと見なされる。すると、時刻同期フレームＰ１は、ゲートウェイ装置ＧＷの時計３３で１３：００にノード装置１Ａにおいて受信される。しかし、時刻同期フレームＰ１を受信したときのノード装置１Ａの時計３３は、例えば、１２：５８を示して

いるかもしれないし、１３：０３を示しているかもしれない。

【０２０８】

そこで、時刻同期フレームＰ１を受信したノード装置１Ａは、ノード装置１Ａ自身の時計３３の時刻合わせ（すなわち時刻同期処理）をステップＳ７０３で行う。その結果、ノード装置１Ａの時計３３は、１３：００に補正される。なお、ステップＳ７０３の時刻同期処理は、具体的には、図２１の時刻同期フレーム受信処理である。

【０２０９】

ステップＳ７０３においてノード装置１Ａの時計３３が補正されるということは、換言すれば、ステップＳ７０３でノード装置１Ａが、時間帯Ｔｎａ１から時間帯Ｔｎａ２にスイッチしたとも言える。

【０２１０】

また、個々のノード装置１Ａ～１Ｃは、個々のスケジュール設定に応じて時刻同期フレーム送信処理を行う。例えば、図１９の例では、ノード装置１Ｂが、ノード装置１Ｂの時計で１３：３０になると、ステップＳ７０４に示すように、時刻同期フレームＰ２を送信する。時刻同期フレームＰ２は、「同期時刻が１０：００で現在時刻が１３：３０である」と示している。また、時刻同期フレームＰ２のローカル宛先アドレスはノード装置１Ａのアドレスであるとする。

【０２１１】

すると、ノード装置１Ａは、時刻同期フレームＰ２を受信し、時刻同期フレームＰ２の受信を契機として、ステップＳ７０５に示すように時刻同期処理を行う。しかし、既にステップＳ７０３で行った時刻同期処理で使われた時刻同期フレームＰ１に同期時刻として示されていた１２：００よりも、時刻同期フレームＰ２に同期時刻として示されている１０：００の方が古い。そのため、詳しくは図２１とともに説明するように、ステップＳ７０５では、ノード装置１Ａは時計３３を更新しない。

【０２１２】

ところで、個々のノード装置１Ａ～１Ｃには、時刻同期処理によって時計３３を補正してから、隣接する他のノード装置に時刻同期フレームを送信するまでの間隔Ｔｎａｘが、予め設定されている。例えば、ノード装置１Ａに設定されている間隔Ｔｎａｘは、４０分である。

【０２１３】

個々のノード装置１Ａ～１Ｃごとに、異なるランダムな間隔が設定されていてもよい。また、ノード装置１Ａは、時計３３を補正してから複数のノード装置１Ｂと１Ｃへそれぞれ時刻同期フレームを送信するまでの間隔が、同じ値（例えば上記の間隔Ｔｎａｘ）に設定されていてもよい。あるいは逆に、１つのノード装置１Ａにおいて、時計３３を補正してからノード装置１Ｂへ時刻同期フレームを送信するまでの間隔（図１９には不図示）と、時計３３を補正してからノード装置１Ｃへの時刻同期フレームを送信するまでの間隔Ｔｎａｘとが、異なる値に設定されていてもよい。

【０２１４】

ノード装置１Ａは、設定にしたがって、時計３３を補正してから所定の時間（すなわちＴｎａｘ＝４０分）が経過すると、ステップＳ７０６に示すように時刻同期フレーム送信処理を行う。ステップＳ７０６では、「同期時刻が１２：００で現在時刻が１３：４０である」と示す時刻同期フレームＰ３が送信される。

【０２１５】

時刻同期フレームＰ３が「同期時刻が１２：００」と示すのは、ノード装置１Ａが時計３３を補正する契機となった時刻同期フレームＰ１が、同期時刻として示していたのが１２：００だからである。また、時刻同期フレームＰ３が「現在時刻が１３：４０」と示すのは、時刻同期フレームＰ３が１３：４０に送信されるからである。

【０２１６】

そして、時刻同期フレームＰ３がノード装置１Ｃで受信されると、ステップＳ７０７に示すように、ノード装置１Ｃが時刻同期処理を行う。

図２０は時刻同期フレーム送信処理のフローチャートである。例えば、図１９のステップＳ７０２ではゲートウェイ装置ＧＷが、ステップＳ７０４ではノード装置１Ｂが、ステップＳ７０６ではノード装置１Ａが、それぞれ図２０の処理を行う。

【０２１７】

例えば、ノード装置１Ａの時刻同期部９は、図５のカウンタ３４とは別の不図示の第２のカウンタを備えていてもよい。第２のカウンタは、例えば図４のタイマＩＣ１３と類似のハードウェア回路により実現することができる。

【０２１８】

第２のカウンタには、間隔Ｔｎａｘを示す値が設定される。そして、時刻同期部９は、図２１とともに後述する時刻同期フレーム受信処理の終了時に第２のカウンタをクリアする。第２のカウンタが、間隔Ｔｎａｘを示す値までカウントアップすると、図２０の処理を時刻同期部９が開始する。

【０２１９】

あるいは、時刻同期部９は、時計３３を補正した時刻を記憶し、記憶した時刻から間隔Ｔｎａｘが経過したか否かを、時計３３を参照することにより判断し、間隔Ｔｎａｘが経過していれば図２０の処理を開始してもよい。

【０２２０】

図２０の処理が開始されると、ステップＳ８０１で時刻同期部９は、自ノード装置１で保持している最終同期時刻を、同期時刻としてフレームに設定する。

時刻同期部９は、最後に図２１の処理を行ったときの時刻同期フレームの同期時刻フィールドから得た時刻を、ノード装置１自身における「最終同期時刻」として、例えばＤＲＡＭ１５上に保持している。そこで、ステップＳ８０１では、時刻同期部９は、新たに作成する平文フレームの同期時刻フィールドに、保持している最終同期時刻の値を設定する。

【０２２１】

例えば図１９の例において、ノード装置１Ａの時刻同期部９がステップＳ７０６を実行する場合、時刻同期部９は、ステップＳ７０３で時計３３を補正した契機となった時刻同期フレームＰ１が示す同期時刻である１２：００を、最終同期時刻として保持している。よって、ステップＳ７０６から呼び出された図２０の処理のステップＳ８０１では、時刻同期部９は、新たに作成する平文フレームの同期時刻フィールドに、１２：００と設定する。

【０２２２】

次に、ステップＳ８０２で時刻同期部９は、自ノード装置１の時刻同期フレーム送信時刻を、「現在時刻」としてフレーム（つまり新たに作成する平文フレーム）に設定する。より厳密には、ステップＳ８０２の実行時に時計３３が示す時刻が、近似的に、ノード装置１からの時刻同期フレーム送信時刻であると見なされて、時刻同期部９によって平文フレームの現在時刻フィールドに設定される。

【０２２３】

例えば図１９の例において、ノード装置１Ａの時刻同期部９がステップＳ７０６を実行する場合、ステップＳ７０６から呼び出された図２０の処理のステップＳ８０２では、時刻同期部９は、平文フレームの現在時刻フィールドに、１３：４０と設定する。

【０２２４】

そして、ステップＳ８０３で時刻同期部９は、時刻同期フレームのヘッダを作成し、作成したヘッダを、平文ペイロード（同期時刻と現在時刻を含む）の前に付与する。ステップＳ８０３で作成されるヘッダは、例えば、ハローフレームのアドホックヘッダＤ９と同様の形式である。そして、時刻同期部９は、ヘッダと平文ペイロードからなる平文フレームを時刻同期フレーム暗号化部３８に出力する。

【０２２５】

するとステップＳ８０４で時刻同期フレーム暗号化部３８は、時刻同期鍵格納部３５を参照して時刻同期鍵を読み出し、時刻同期鍵を用いて、平文ペイロードを暗号化する。例

えば、時刻同期フレームの暗号化のための暗号化アルゴリズムもＲＣ４である場合、時刻同期フレーム暗号化部３８は、ステップＳ８０４において、具体的には、鍵ストリームの生成とＸＯＲ操作を行う。時刻同期フレーム暗号化部３８は、ステップＳ８０３で付与したヘッダと、ステップＳ８０４で暗号化したペイロードとからなる時刻同期フレームを、時刻同期フレーム送信バッファ４２に出力する。

【０２２６】

最後にステップＳ８０５で、送信部７が時刻同期フレームを送信する。つまり、送信処理部４４が、時刻同期フレーム送信バッファ４２に一時的に格納された時刻同期フレームを送信し、図２０の処理は終了する。

【０２２７】

図２１は時刻同期フレーム受信処理のフローチャートである。例えば、図１９のステップＳ７０３とＳ７０５では、ノード装置１Ａが図２１の処理を行う。図２１の処理は、ノード装置１が受信部８でフレームを受信し、受信部８のフレーム分岐処理部２１がアドホックヘッダＤ９のフレームタイプＤ７に基づいて「受信したフレームは時刻同期フレームである」と判別することを契機として、開始される。なお、フレーム分岐処理部２１が「受信したフレームは時刻同期フレームである」と判別すると、受信されたフレームは時刻同期フレーム受信バッファ２３に出力され、格納される。

【０２２８】

ステップＳ９０１で時刻同期フレーム復号部２６は、時刻同期フレーム受信バッファ２３から時刻同期フレームを読み出して復号化を行う。すなわち、時刻同期フレーム復号部２６は時刻同期鍵格納部３５を参照して時刻同期鍵を読み出し、時刻同期鍵を用いて、時刻同期フレームの暗号化されているペイロードを復号する。

【０２２９】

上記のように時刻同期フレームの暗号化のための暗号化アルゴリズムもＲＣ４である場合、時刻同期フレーム復号部２６は、ステップＳ９０１において、具体的には、鍵ストリームの生成とＸＯＲ操作を行う。

【０２３０】

また、復号後、時刻同期フレーム復号部２６は、ヘッダと、復号によって得た平文ペイロードとを時刻同期部９に出力する。

すると、ステップＳ９０２で時刻同期部９は、平文ペイロードから同期時刻フィールドの値を抽出するとともに、例えばＤＲＡＭ１５に保持している最終同期時刻を読み出す。そして時刻同期部９は、抽出した同期時刻と読み出した最終同期時刻を比較する。

【０２３１】

同期時刻が最終同期時刻よりも新しいとき、処理はステップＳ９０３に移行する。逆に、同期時刻が最終同期時刻と同じか、又は同期時刻が最終同期時刻よりも古いとき、処理はステップＳ９０４に移行する。

【０２３２】

ステップＳ９０３で時刻同期部９は、時刻同期フレームの現在時刻を、自ノード装置１の時刻として設定する。すなわち、時刻同期部９は、時刻同期フレームの現在時刻フィールドの値を抽出し、抽出した値を時計３３に設定することで、時計３３の時刻を補正する。そして、図２１の処理は終了する。

【０２３３】

例えば、図１９のステップＳ７０３から図２１の処理が呼び出された場合、ステップＳ９０３が実行され、時刻同期部９が時計３３を補正する。

また、ステップＳ９０４では、時刻同期部９は時刻同期フレームを破棄し、図２１の処理が終了する。例えば、図１９のステップＳ７０５から図２１の処理が呼び出された場合、ステップＳ９０４が実行される。

【０２３４】

なお、図２０及び図２１に関して説明したように、本実施形態の時刻同期フレームには特に署名などのトレイラは含まれないが、平文ペイロードのハッシュ値をトレイラとして

付与したフォーマットの時刻同期フレームを利用する実施形態も可能である。

【０２３５】

その場合、時刻同期フレーム送信処理において、時刻同期部９はハッシュ値の計算を行い、時刻同期フレーム暗号化部３８はペイロードとトレイラの双方を暗号化する。また、時刻同期フレーム受信処理において、時刻同期フレーム復号部２６はペイロードとトレイラの双方を復号する。そして、確認部２９が、復号により得られた平文ペイロードからハッシュ値を計算し、計算したハッシュ値と復号により得られた平文ハッシュ値とを比較し、２つのハッシュ値が一致する場合のみ、時刻同期部９がステップＳ９０２以降の処理を実行する。

【０２３６】

アドホック通信ネットワークを構成するノード装置数が多い場合に、ゲートウェイ装置等の所定の１つの装置の時刻に各ノード装置が同期をとる構成では、トラフィックが増大することとなる。他方、本実施形態によれば、ノード装置数が多い場合であっても、上記の時刻同期方法のように、各ノード装置が、隣接するノード装置のうち既に同期をとったノード装置から時刻同期フレームを受信して時刻合わせを行う。そのため、本実施形態によれば、ネットワーク全体としてのトラフィックを増大させることなく、各ノード装置が時刻の同期をとることができる。

【０２３７】

以上、図１～図２１を参照して本実施形態について詳しく説明したが、本実施形態のノード装置１について概観すれば下記のごとくである。

図３～図５に示すノード装置１は、例えば図２、図６、図７、図１８及び図１９に示すように複数のノード装置によって構成されるネットワークの中のノード装置の１つである。ここで説明の便宜上、複数のノード装置のうち第１のノード装置１Ａと第２のノード装置１Ｂに注目し、第１のノード装置１Ａの構成について概観する。

【０２３８】

第１のノード装置１Ａは、図３及び図５に示すように、第１のノード装置１Ａ固有の暗号鍵である第１のアクセスキーを、第１の時間ごとに変更して生成するアクセスキー生成部２を有する。ここで、「第１のアクセスキー」とは、例えば、図６のアクセスキーａ１であり、「第１の時間」とは、上記実施形態の例ではt_1＝１０（分）である。

【０２３９】

また、第１のノード装置１Ａは、図３及び図５に示すように、ネットワーク内の複数のノード装置で共通の共通鍵を、複数のノード装置で共通の時間である第２の時間ごとに変更して生成する共通鍵生成部３を有する。ここで、「第２の時間」とは、上記実施形態の例ではt_2＝１２（時間）である。

【０２４０】

また、第１のノード装置１Ａは、生成された第１のアクセスキーを、生成された共通鍵で暗号化して第２のノード装置１Ｂに送信するアクセスキー通知部として働くコンポーネントを有する。すなわち、図３のフレーム処理部６と暗号化部４と送信部７が、協働して上記アクセスキー通知部として働く。より詳しくは、図５のハローフレーム作成部３６とハローフレーム暗号化部３７とハローフレーム送信バッファ４１と送信処理部４４が、協働して上記アクセスキー通知部として働く。

【０２４１】

また、第１のノード装置１Ａは、第２のノード装置１Ｂから送信されてきたアクセスキー通知フレームを受信するアクセスキー受信部として働くコンポーネントを有する。ここで、「アクセスキー通知フレーム」とは、第２のノード装置１Ｂに固有の暗号鍵である第２のアクセスキーを共通鍵で暗号化したデータであるアクセスキー通知データを含み、具体的には、上記実施形態における、暗号化されたハローフレームである。また、「第２のアクセスキー」は、例えば図６のアクセスキーｂ１であり、「アクセスキー通知データ」は、例えば図１２の暗号化アクセスキーＤ３である。

【０２４２】

なお、上記実施形態では、図３の受信部８（より詳しくは図５のフレーム分岐処理部２１とハローフレーム受信バッファ２２）がアクセスキー受信部として働く。

また、第１のノード装置１Ａは、アクセスキー通知データを、生成された共通鍵を用いて復号することにより、アクセスキー通知データから第２のアクセスキーを取得するアクセスキー復号化部として働くコンポーネントを有する。すなわち、上記実施形態では、図３の復号部５（より詳しくは図５のハローフレーム復号部２５）が、上記アクセスキー復号化部として働いて、アクセスキーｂ１を取得する。

【０２４３】

また、第１のノード装置１Ａは、データ送信部として働くコンポーネントを有する。データ送信部は、第１の平文フレームに、第１の平文フレームから計算される第１のハッシュ値を含むデータを共通鍵で暗号化した第１の署名データを付与する。そして、データ送信部は、第１の署名データの付与された第１の平文フレームを、復号して得た第２のアクセスキーで暗号化して、第１の暗号化フレームとして送信する。

【０２４４】

ここで「第１の平文フレーム」の例は、図１５に関して説明した、アドホックヘッダＤ９と、平文ＦＩＤ・Ｄ１５と平文ボディＤ１６からなる平文ペイロードとを含む、平文フレームである。「第１のハッシュ値」の例は、まだトレイラが作成されていない平文フレームから（より正確には平文ペイロードから）計算される、図１５の平文ハッシュ値Ｄ１７であり、「第１の署名データ」の例は暗号化署名Ｄ２１である。実施形態によっては、ハッシュ値の計算にさらにヘッダが利用されてもよい。また、「第２のアクセスキー」は、具体的には、図６のアクセスキーｂ１である。

【０２４５】

上記実施形態では、図３の暗号化部４と送信部７（より詳しくは、図５のデータフレーム暗号化部３９とデータフレーム送信バッファ４３と送信処理部４４）が、協働して上記データ送信部として働く。

【０２４６】

また、第１のノード装置１Ａは、第２のノード装置１Ｂから第２の暗号化フレームを受信するデータ受信部として働く図３の受信部８（より詳しくは図５のフレーム分岐処理部２１とデータフレーム受信バッファ２４）を有する。ここで、「第２の暗号化フレーム」とは、第２の平文フレームが第１のアクセスキーにより暗号化されたフレームであり、「第２の平文フレーム」とは、第２のハッシュ値を含むデータを前記共通鍵で暗号化した第２の署名データが付与されたフレームである。

【０２４７】

また、第１のノード装置１Ａは、データ復号化部として働く図３の復号部５（より詳しくは図５のデータフレーム復号部２７）を有する。上記データ復号化部は、第２の暗号化フレームを第１のアクセスキーで復号して、第２の暗号化フレームから、第２の署名データが付与された第２の平文フレームを得る。

【０２４８】

上記実施形態の説明においては、図１５の例を、ノード装置１Ａからノード装置１Ｂへのデータフレームの送信の場合に即して説明したが、図１５は、ノード装置１Ｂからノード装置１Ａへのデータフレームの送信の場合にも当てはまる。この場合、ノード装置１Ｂから送信されてきた「第２の暗号化フレーム」に相当するのは、図１５のアドホックヘッダＤ９とペイロードＤ２６とトレイラＤ２７からなるデータフレームである。

【０２４９】

そして、上記データ復号化部として働くノード装置１Ａのデータフレーム復号部２７は、「第１のアクセスキー」であるアクセスキーａ１を用いて、第２の平文フレームを得る。ここで、「第２の平文フレーム」は、アドホックヘッダＤ９と、復号された平文ＦＩＤ・Ｄ２８及び復号された平文ボディＤ２９からなる平文ペイロードとを含む。また、「第２の平文フレーム」には、復号された暗号文ハッシュ値Ｄ３０と復号された暗号文時刻Ｄ３１からなる暗号化署名（上記の「第２の署名データ」に相当）が、トレイラとして付与

されている。

【０２５０】

また、第１のノード装置１Ａは、整合性確認部として働くコンポーネントを有する。上記実施形態では図５のデータフレーム復号部２７と確認部２９が協働して整合性確認部として働く。具体的には、整合性確認部の一部としてのデータフレーム復号部２７が、生成された共通鍵を用いて第２の署名データを復号することにより第２のハッシュ値を取得する。そして、整合性確認部の一部としての確認部２９が、第２の平文フレームから第３のハッシュ値（例えば図１５の計算されたハッシュ値Ｄ３２）を計算し、第２のハッシュ値と前記第３のハッシュ値との整合性が取れているか否かを確認する。

【０２５１】

なお、上記のデータ送信部は、さらに、第１の平文フレーム中に、第１の平文フレームを一意に識別するための第１の識別子と、第１の送信時刻を示す情報とを含ませてもよい。

【０２５２】

上記実施形態では、データフレーム作成部４０もデータ送信部の一部として働いており、データフレーム作成部４０が、「第１の識別子」としての図１７の平文ＦＩＤ・Ｄ１５と「第１の送信時刻を示す情報」としての平文時刻Ｄ１８を、第１の平文フレーム中に含ませる。あるいは、データフレーム作成部４０が、「第１の送信時刻を示す情報」として、図１５のように暗号化時刻Ｄ２０を、第１の平文フレーム中に含ませてもよい。平文時刻Ｄ１８と暗号化時刻Ｄ２０は、クリアテキストか暗号文かという違いはあるが、「第１の送信時刻を示す」という点では同じである。

【０２５３】

また、図５の受信データフレーム処理部３０が、さらに上記の整合性確認部として付加的に働いてもよい。つまり、整合性確認部としての受信データフレーム処理部３０は、第２の暗号化フレームから復号された第２の平文フレームに含まれる第２の識別子が、過去に受信したことのある第３の暗号化フレームから復号した第３の平文フレームに含まれる第３の識別子と等しい場合に、第２と第３の平文フレームのうち、復号により得られる情報がより新しい送信時刻を示す方を破棄してもよい。

【０２５４】

例えば、図１７の例をノード装置１Ｂからノード装置１Ａへの送信の場合に当てはめると、「第２の平文フレーム」は、アドホックヘッダＤ９と、平文ペイロードと、平文トレイラとしての復号された暗号文ハッシュ値Ｄ４６とからなる。そして、平文ペイロードは、復号された平文ＦＩＤ・Ｄ４３、復号された平文時刻Ｄ４４及び復号された平文ボディＤ４５からなる。また、「第２の識別子」は復号された平文ＦＩＤ・Ｄ４３に相当する。

【０２５５】

そして、整合性確認部としての受信データフレーム処理部３０は、次のように動作する。すなわち、受信データフレーム処理部３０は、平文ＦＩＤ・Ｄ４３が、過去に受信したことのある他のデータフレームのＦＩＤと等しい場合、復号により得られる送信時刻（例えば、復号された平文時刻Ｄ４４）が新しい方のデータフレームを破棄する。

【０２５６】

このように、データ送信部及び整合性確認部としての各部が、識別子（具体的にはＦＩＤ）を使った処理を行うことで、ノード装置１Ａは、不正なノード装置から送信されたフレームを検出することができる。

【０２５７】

また、ネットワーク内の複数のノード装置（例えばノード装置１Ａと１Ｂを含む）のそれぞれの共通鍵生成部３は、上記のように、共通の時間である第２の時間ごとに共通鍵を生成する。したがって、複数のノード装置それぞれの時計（例えば図５の時計３３）が、無視しても問題ない程度の誤差の範囲内で互いに同期していれば、複数のノード装置で共通鍵が生成されるタイミングも同期していることになる。

【０２５８】

しかしながら、複数のノード装置それぞれの時計の時刻のずれが時とともに拡大することもありうる。そこで、上記実施形態は、複数のノード装置それぞれの時計の時刻のずれを補正することで、ネットワーク内の複数のノード装置間で、共通鍵を生成するタイミングの同期をとっている。

【０２５９】

すなわち、第１のノード装置１Ａは、協働して時刻同期フレーム送信部として働くコンポーネントを有する。時刻同期フレーム送信部は、時刻同期フレームとして、第１のノード装置１Ａにおける第１の現在時刻と、第１のノード装置１Ａにおいて時刻合わせを行った第１の同期時刻とを示すデータを含んだ第１の時刻同期フレームを生成して送信する。

【０２６０】

例えば、図１９の例では、ステップＳ７０３以降における「第１の同期時刻」は１２：００であり、ステップＳ７０６では「第１の現在時刻」として１３：４０を示す情報を含む時刻同期フレームＰ３が送信されている。

【０２６１】

なお、上記実施形態の時刻同期フレームは時刻同期鍵により暗号化されているが、時刻同期フレームが暗号化されない実施形態も可能である。したがって、上記実施形態では図５の時刻同期部９、時刻同期フレーム暗号化部３８、時刻同期フレーム送信バッファ４２及び送信処理部４４が、協働して時刻同期フレーム送信部として働いているが、時刻同期フレーム暗号化部３８が省略されてもよい。

【０２６２】

また、第１のノード装置１Ａは、第２の時刻同期フレームを第２のノード装置１Ｂから受信する時刻同期フレーム受信部として働くコンポーネントを有する。ここで、第２の時刻同期フレームは、第２のノード装置１Ｂにおける第２の現在時刻（例えば図１９の例では１３：３０）と、前記第２のノード装置において時刻合わせを行った第２の同期時刻（例えば図１９の例では１０：００）とを示すデータを含む。

【０２６３】

上記実施形態では図５のフレーム分岐処理部２１及び時刻同期フレーム受信バッファ２３が、協働して上記時刻同期フレーム受信部として働く。

さらに、第１のノード装置１Ａは、時刻更新部として働くコンポーネントを有する。時刻更新部は、第２の時刻同期フレームから得られる第２の同期時刻と、第１のノード装置１Ａが記憶している第１の同期時刻とを比較する。そして、第２の同期時刻の方が新しければ、時刻更新部は、第２の現在時刻を第１のノード装置１Ａにおける現在時刻として設定して、第１のノード装置１Ａの時刻を更新する。

【０２６４】

具体的には、図５の時刻同期部９が時刻更新部として働く。また、上記実施形態では、時刻同期フレームが暗号化されているので、第２の時刻同期フレームから第２の同期時刻を得るため、時刻同期フレーム復号部２６も時刻更新部の一部として働いている。

【０２６５】

そして、ノード装置１Ａは、記憶部として、例えばＤＲＡＭ１５を有する。当該記憶部は、時刻更新部としての時刻同期部９が第１のノード装置１Ａの時刻を更新することで時刻合わせを行った時刻として、第２の同期時刻を記憶する。また、図３及び図５の共通鍵生成部３は、時刻更新部としての時刻同期部９が更新した時刻（具体的には図５の時計３３が示す時刻）に基づいて第２の時間を計時する。

【０２６６】

以上概観した上記実施形態によれば、第２のノード装置が正当なノード装置である場合には、第２のノード装置は、第１のノード装置と共通する共通鍵を保有している。よって、第１のノード装置で生成した第１のアクセスキーと、第２のノード装置で生成した第２のアクセスキーは、共通鍵を用いてセキュアに交換することができる。

【０２６７】

また、第１のノード装置は、復号して得られた第２のノード装置の第２のアクセスキー

を用いてデータを暗号化して第２のノード装置に送信することが可能である。さらに、第１のノード装置は、第２のノード装置からは、第１のノード自身が生成した第１のアクセスキーを用いて暗号化されたデータを受信することも可能である。

【０２６８】

このように、上記実施形態によれば、各ノード装置が、暗号化のための動作を自律的に他のノード装置と協働して行う。したがって、非常に多くのノード装置を含むネットワークにおいても、暗号化鍵の交換のためのトラフィックが集中することはない。

【０２６９】

また、各ノード装置が、暗号化のための動作を自律的に行うためには、各ノード装置が時間に応じて生成しなおして変更する共通鍵の、変更タイミングの同期をとることが求められる。上記の実施形態によれば、簡易な構成で、かつ、ネットワークに負荷をかけずに、自律的に共通鍵を、同期をとって変更可能なノード装置が提供される。

【０２７０】

なお、上記の実施形態においては、ノード装置について主に説明したが、上記の方法をコンピュータに実行させる制御プログラムも、本発明の実施形態の一例に含まれる。当該制御プログラムは、磁気ディスク、光磁気ディスク、不揮発性の半導体メモリ、光ディスクなどの、コンピュータ読み取り可能な記憶媒体に格納されて提供され、コンピュータにロードされ、コンピュータにより実行されてもよい。

【０２７１】

当該制御プログラムを実行するコンピュータは、不図示のノード装置に内蔵又は接続され、上記不図示のノード装置が上記実施形態のノード装置１と同様に動作するように、当該制御プログラムにしたがって上記不図示のノード装置を制御する。例えば、上記実施形態を別の観点から見れば、ノード装置１の内蔵コンピュータであるＭＰＵ１１は、フラッシュメモリ１６に格納された制御プログラムにしたがってノード装置１を制御し、上記各処理をノード装置１に行わせている、とも言える。

【０２７２】

また、上記実施形態で例示したＲＣ４は、採用可能な暗号化アルゴリズムの一例である。実施形態によっては、その他の暗号化アルゴリズムによる暗号化及び復号が行われてもよい。例えば、ストリーム暗号以外の暗号化アルゴリズムが使われてもよい。また、時刻同期鍵、共通鍵、アクセスキーそれぞれを使った暗号化及び復号が、異なる暗号化アルゴリズムによるものであってもよい。

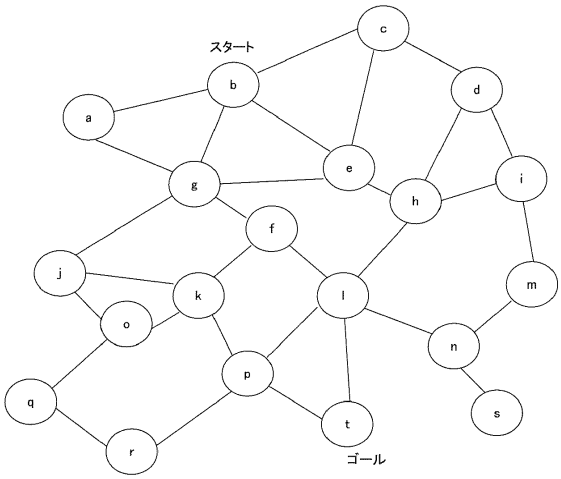
【０２７３】

また、ハローフレーム、データフレーム、時刻同期フレームのフォーマットは、上記実施形態で例示したものに限らないことは無論である。例えば、各フレームは、上記実施形態では例示していないフィールドをさらに含んでいてもよい。逆に、フレームが固定長であれば、フレームサイズＤ８のフィールドは省略可能である。

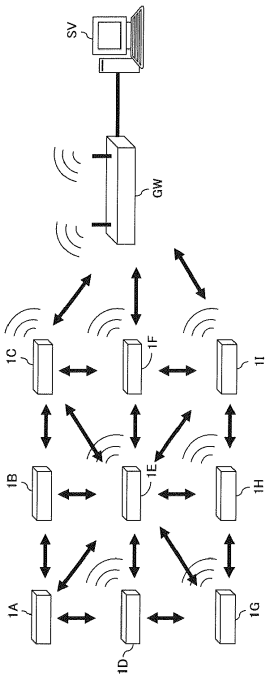
【０２７４】

さらに、上記実施形態で例示した「１０分」などの具体的な数値は、理解の助けとするために示したに過ぎず、実施形態によって具体的数値は様々に設定されてよい。

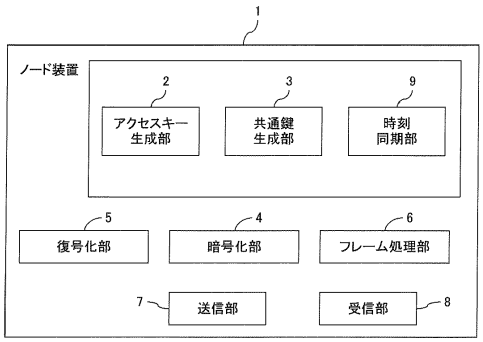
【図１】


スタート
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
ゴール

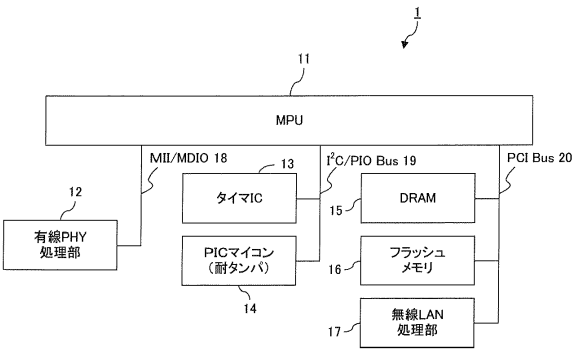
【図２】


SV
GW
1A
1B
1C
1D
1E
1F
1G
1H
1I

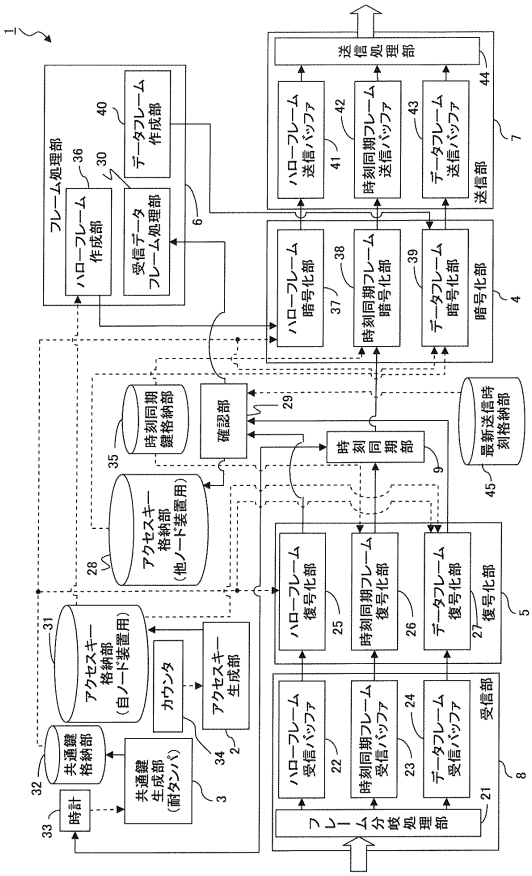
【図３】


1
ノード装置
2
アクセスキー生成部
3
共通鍵生成部
9
時刻同期部
5
復号化部
4
暗号化部
6
フレーム処理部
7
送信部
受信部
8

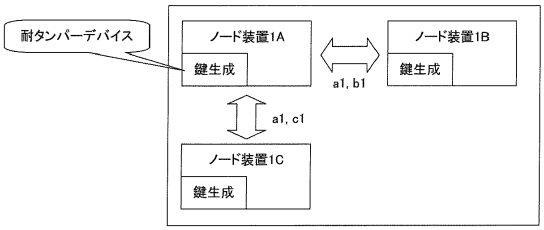
【図４】


1
11
MPU
MII/MDIO 18
I²C/PIO Bus 19
PCI Bus 20
12
有線PHY処理部
13
タイマIC
15
DRAM
PICマイコン（耐タンパ）
14
16
フラッシュメモリ
17
無線LAN処理部

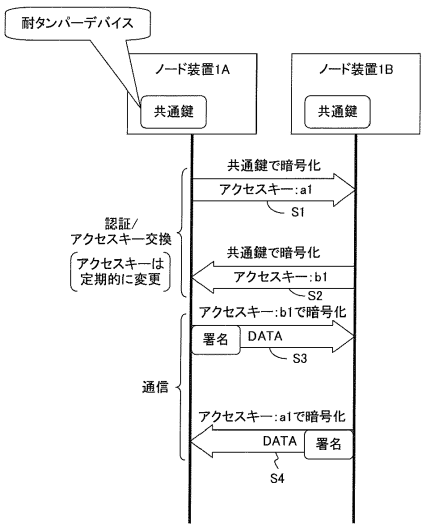
【図５】



【図６】



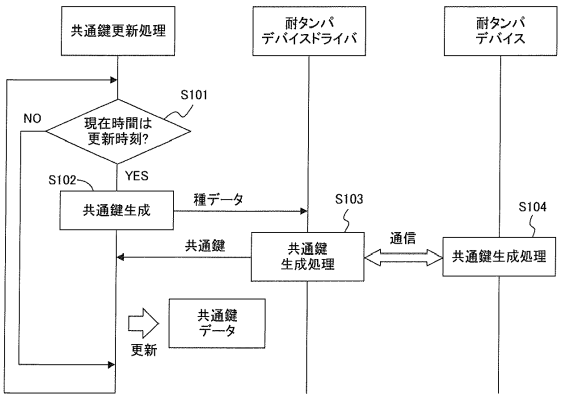
【図７】



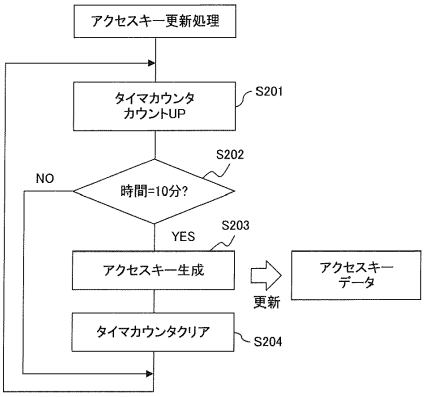
【図８】

Frame				署名
ヘッダ	FID	時刻	ボディ	Kt(Hash(Frame))

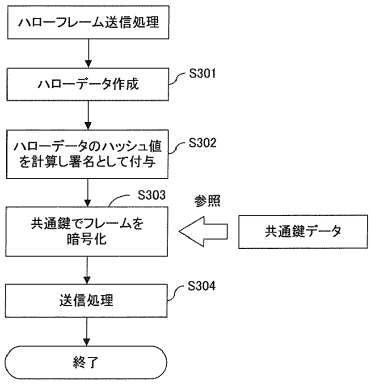
【図９】



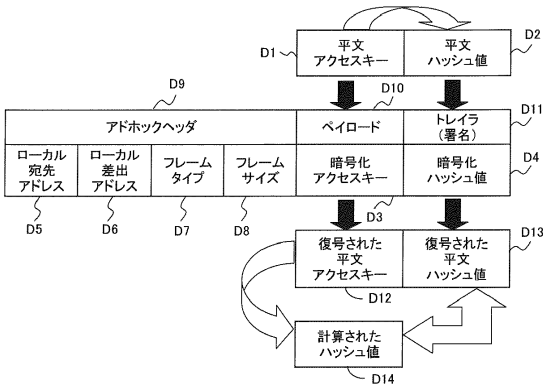
【図１０】



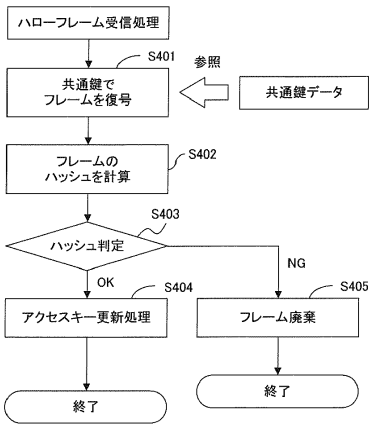
【図１１】



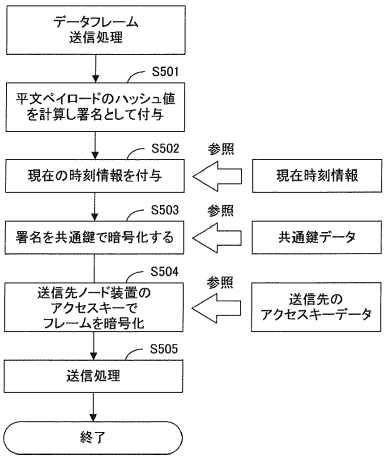
【図１２】



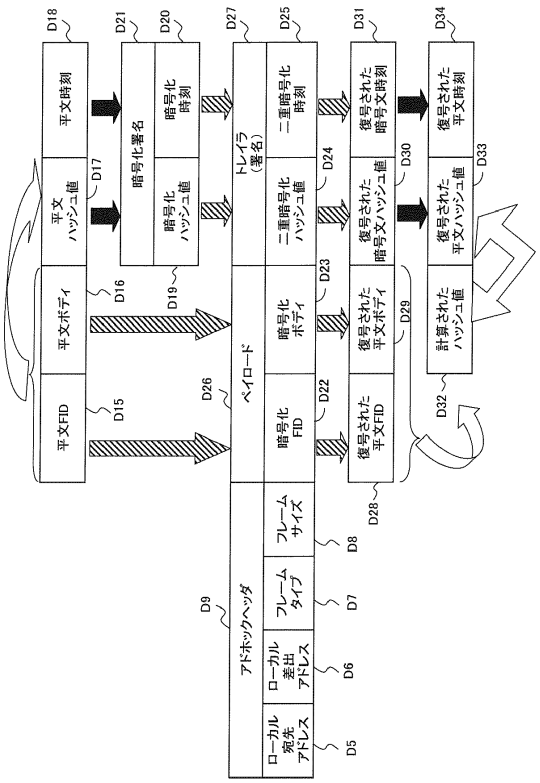
【図１３】



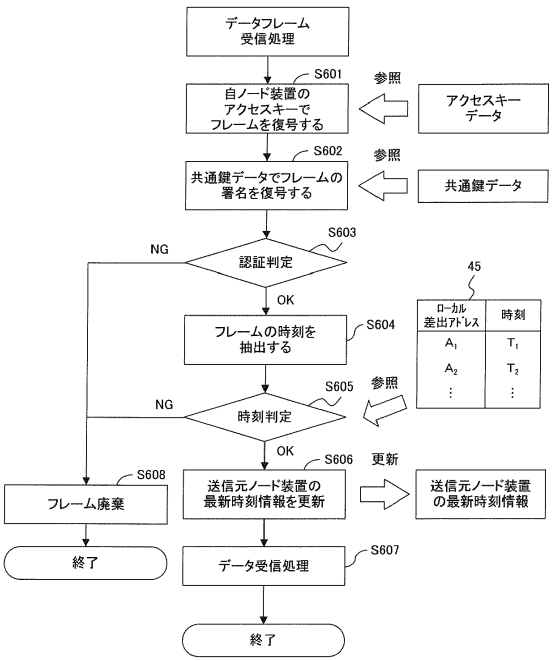
【図１４】



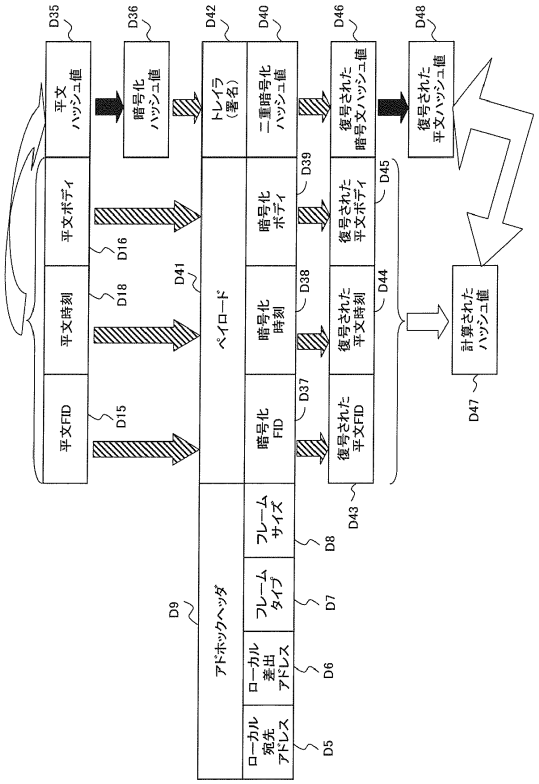
【図１５】



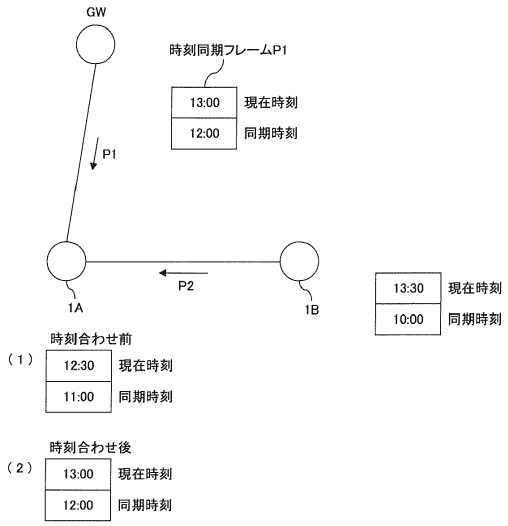
【図１６】



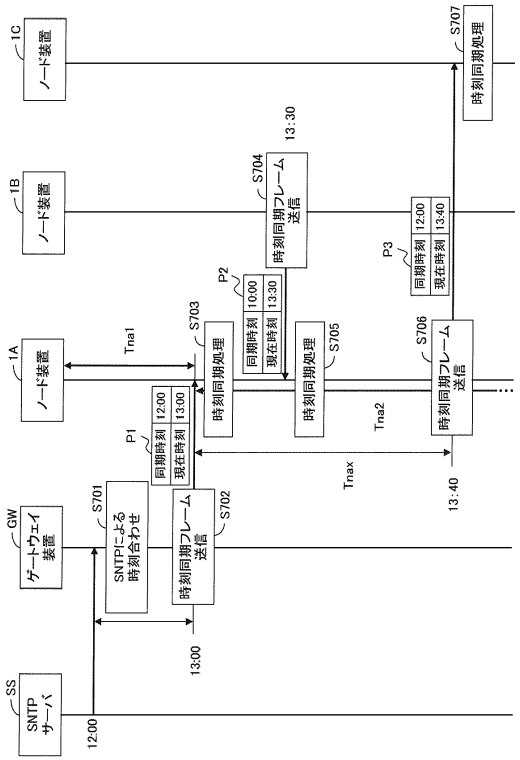
【図１７】



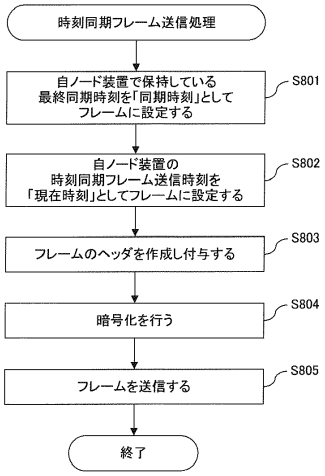
【図１８】



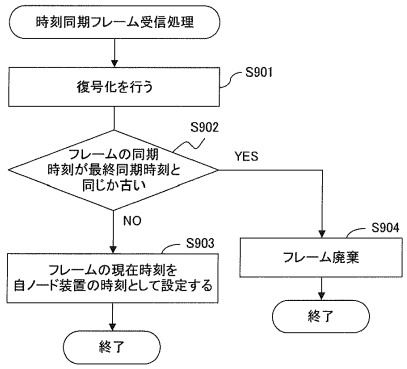
【図１９】



【図２０】



【図２１】


時刻同期フレーム受信処理
復号化を行う
S901
S902
フレームの同期
時刻が最終同期時刻と
同じか古い
YES
NO
S903
フレームの現在時刻を
自ノード装置の時刻として設定する
終了
S904
フレーム廃棄
終了

フロントページの続き

(72)発明者　中嶋　千明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　池本　健太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　古賀　俊介
福岡県福岡市早良区百道浜２丁目２番１号　富士通九州ネットワークテクノロジーズ株式会社内
(72)発明者　高橋　勇治
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　金沢　史明

(56)参考文献　特開２００４－３４３７１７（ＪＰ，Ａ）
特開２００５－２７８０４４（ＪＰ，Ａ）
特開２００７－１０４３１０（ＪＰ，Ａ）
特開２００２－１１１６７９（ＪＰ，Ａ）
特開２００６－５１４７８９（ＪＰ，Ａ）
特開２００４－５６７６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08