(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4197031号
(P4197031)
(45)発行日　平成20年12月17日(2008.12.17)　(24)登録日　平成20年10月10日(2008.10.10)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A

請求項の数 26　(全 38 頁)

(21)出願番号　特願2006-324059(P2006-324059)
(22)出願日　平成18年11月30日(2006.11.30)
(65)公開番号　特開2008-141360(P2008-141360A)
(43)公開日　平成20年6月19日(2008.6.19)
審査請求日　平成18年11月30日(2006.11.30)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１８年度新エネルギー・産業技術総合開発機構「デジタル情報機器の統合リモート管理基盤技術の研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

(73)特許権者　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(72)発明者　八百　健嗣
東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】メッセージ認証システム及びメッセージ認証方法

(57)【特許請求の範囲】
【請求項１】
マルチホップ型ネットワークにおいて、メッセージを送信するメッセージ送信装置と、送信されたメッセージの認証を行うメッセージ受信装置とを備えるメッセージ認証システムにおいて、
前記メッセージ送信装置は、
メッセージの認証に用いられる２以上の認証子生成鍵を含む認証子生成鍵鎖列を管理する認証子生成鍵管理部と、
前記認証子生成鍵を用いて、前記メッセージの正当性を証明するための第１認証子及び前記第１認証子の正当性を証明するための第２認証子からなる送信予告情報を生成する送信予告情報生成部と、
前記送信予告情報を前記メッセージ受信装置に送信し、前記送信予告情報に対応して前記メッセージ受信装置から送信される受信証明情報を認証した後で、前記メッセージと前記認証子生成鍵とを送信する送信部と、
を含み、
前記メッセージ受信装置は、
前記送信予告情報の受信を証明する受信証明情報を生成する受信証明情報生成部と、
前記第２認証子と前記メッセージ送信装置から送信された前記認証子生成鍵とを用いて前記第１認証子の認証を行う第１認証子認証部と、
前記認証された第１認証子と前記認証子生成鍵とを用いて、前記メッセージ送信装置か

ら受信した前記メッセージの認証を行うメッセージ認証部と、
を含むことを特徴とする、メッセージ認証システム。
【請求項２】
前記認証子生成鍵管理部は、任意の値に対し、公開された一方向性関数を実行する回数を順次増加させることにより前記各認証子生成鍵を生成し、生成された順と逆の順序で前記各認証子生成鍵を前記メッセージ受信装置に対して公開することを特徴とする、請求項１に記載のメッセージ認証システム。
【請求項３】
前記送信予告情報生成部は、未公開の前記認証子生成鍵、または前記未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかを用いて、前記第１認証子を生成することを特徴とする、請求項２に記載のメッセージ認証システム。
【請求項４】
前記送信予告情報生成部は、未公開の前記認証子生成鍵、または前記未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかと、前記第１認証子とを用いて、前記第２認証子を生成することを特徴とする、請求項２または３のいずれかに記載のメッセージ認証システム。
【請求項５】
前記メッセージ受信装置は、受信した前記認証子生成鍵が未公開であるか否かを検証し、前記認証子生成鍵が未公開であれば、当該認証子生成鍵を用いて前記第１認証子の認証を行うことを特徴とする、請求項２～４のいずれかに記載のメッセージ認証システム。
【請求項６】
前記メッセージ受信装置は、前記メッセージ送信装置から前記認証子生成鍵が送信されるまで、受信した前記送信予告情報を受信順に保持する送信予告情報保持部をさらに含み、
前記第１認証子認証部は、前記送信予告情報保持部に保持されている前記送信予告情報に含まれる前記第１認証子を受信順に認証し、認証される場合、前記送信予告情報保持部に保持された他の前記送信予告情報を破棄し、認証されない場合、当該送信予告情報を破棄することを特徴とする、請求項１～５のいずれかに記載のメッセージ認証システム。
【請求項７】
前記メッセージ送信装置は、前記メッセージを２以上のデータブロックに分割して送信することを特徴とする、請求項１～６のいずれかに記載のメッセージ認証システム。
【請求項８】
前記送信予告情報生成部は、前記各データブロックに対応する前記送信予告情報を生成し、
前記メッセージ認証部は、前記各データブロックに対応する前記送信予告情報を用いて前記各データブロックを認証することを特徴とする、請求項７に記載のメッセージ認証システム。
【請求項９】
前記送信予告情報生成部は、分割前の前記メッセージに対応する前記送信予告情報を生成し、
前記メッセージ認証部は、前記メッセージの全ての前記データブロックを結合して前記メッセージを復元し、復元された前記メッセージを前記送信予告情報を用いて認証することを特徴とする、請求項７に記載のメッセージ認証システム。
【請求項１０】
前記メッセージ送信装置は、認証情報を前記各データブロックに付加する認証情報付加部をさらに含み、
前記認証情報付加部は、公開された所定の一方向性関数を任意の前記データブロックに適用して前記認証情報を生成し、生成された前記認証情報を他の前記データブロックに付加し、前記認証情報が付加されたデータブロックに前記一方向性関数を適用することを繰り返して前記認証情報を生成することを特徴とする、請求項７に記載のメッセージ認証シ

ステム。
【請求項１１】
前記一方向性関数は、ハッシュ関数であることを特徴とする、請求項１０に記載のメッセージ認証システム。
【請求項１２】
前記送信予告情報生成部は、最後に生成された前記認証情報である第１認証情報に対応する前記送信予告情報を生成し、
前記送信部は、前記データブロックの送信前に前記第１認証情報と前記認証子生成鍵とを前記メッセージ受信装置に対して送信し、前記メッセージ受信装置から前記第１認証情報が認証された旨の通知を受け取った後、前記データブロックを送信し、
前記メッセージ受信装置は、
前記送信予告情報及び前記認証子生成鍵を用いて前記第１認証情報の認証を行う認証情報認証部をさらに含むことを特徴とする、請求項１０または１１のいずれかに記載のメッセージ認証システム。
【請求項１３】
前記送信部は、前記認証情報を生成するのに用いられたのと逆の順序で、前記データブロックを送信し、
前記メッセージ認証部は、前記データブロックの直前に受信したデータブロックに含まれる前記認証情報を用いて前記データブロックの認証を行うことを特徴とする、請求項１０～１２のいずれかに記載のメッセージ認証システム。
【請求項１４】
マルチホップ型ネットワークによってメッセージ送信装置から送信されたメッセージをメッセージ受信装置において認証するメッセージ認証方法において、
メッセージ送信装置からメッセージ受信装置に送信するメッセージを生成するメッセージ生成ステップと、
前記メッセージ送信装置において、メッセージの認証に用いられる２以上の認証子生成鍵を含む認証子生成鍵鎖列を生成する認証子生成鍵生成ステップと、
前記メッセージ送信装置において、前記認証子生成鍵を用いて前記メッセージの正当性を証明するための第１認証子及び前記第１認証子の正当性を証明するための第２認証子を含む送信予告情報を生成する送信予告情報生成ステップと、
前記メッセージ送信装置から前記メッセージ受信装置に対し、前記送信予告情報を送信する送信予告情報送信ステップと、
前記メッセージ受信装置において前記送信予告情報を受信したことを証明する受信証明情報を生成する受信証明情報生成ステップと、
前記メッセージ受信装置から送信される前記受信証明情報を前記メッセージ送信装置が認証する受信証明情報認証ステップと、
前記メッセージ送信装置から前記メッセージ受信装置に対し、前記認証子生成鍵を送信する認証子生成鍵送信ステップと、
前記メッセージ送信装置から前記メッセージ受信装置に対し、前記メッセージを送信するメッセージ送信ステップと
前記第２認証子及び前記メッセージ送信装置から送信された前記認証子生成鍵を用いて、前記メッセージ受信装置が前記第１認証子の認証を行う第１認証子認証ステップと、
前記認証された第１認証子及び前記認証子生成鍵を用いて、前記メッセージ受信装置が前記メッセージ送信装置から受信した前記メッセージの認証を行うメッセージ認証ステップと、
を含むことを特徴とする、メッセージ認証方法。
【請求項１５】
前記送信予告情報生成ステップは、公開された任意の値に対し、公開された一方向性関数を実行する回数を順次増加させることにより前記各認証子生成鍵を生成し、
前記認証子生成鍵鎖列に含まれる前記各認証子生成鍵は、生成順と逆の順序で前記メッ

セージ受信装置に対して公開されることを特徴とする、請求項１４に記載のメッセージ認証方法。

【請求項１６】

前記送信予告情報生成ステップにおいて、未公開の前記認証子生成鍵、または前記未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかを用いて、前記第１認証子を生成することを特徴とする、請求項１５に記載のメッセージ認証方法。

【請求項１７】

前記送信予告情報生成ステップにおいて、未公開の前記認証子生成鍵、または前記未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかと、前記第１認証子とを用いて、前記第２認証子を生成することを特徴とする、請求項１５または１６のいずれかに記載のメッセージ認証方法。

【請求項１８】

前記第１認証子認証ステップの前に、メッセージ受信装置は、受信した前記認証子生成鍵が未公開であるか否かを検証し、前記認証子生成鍵が未公開であれば、当該認証子生成鍵を用いて前記第１認証子の認証を行うことを特徴とする、請求項１５～１７のいずれかに記載のメッセージ認証方法。

【請求項１９】

前記メッセージ受信装置は、前記メッセージ送信装置から前記認証子生成鍵が送信されるまで、受信した前記送信予告情報を受信順に保持し、

前記第１認証子認証ステップにおいて、前記保持されている送信予告情報に含まれる前記第１認証子を受信順に認証し、認証される場合、他の前記送信予告情報を破棄し、認証されない場合、当該送信予告情報を破棄することを特徴とする、請求項１４～１８のいずれかに記載のメッセージ認証方法。

【請求項２０】

前記メッセージ生成ステップにおいて、前記メッセージを２以上のデータブロックに分割して生成することを特徴とする、請求項１４～１９のいずれかに記載のメッセージ認証方法。

【請求項２１】

前記送信予告情報生成ステップにおいて、前記各データブロックに対応する前記送信予告情報を生成し、

前記メッセージ認証ステップにおいて、前記各データブロックに対応する前記送信予告情報を用いて前記各データブロックを認証することを特徴とする、請求項２０に記載のメッセージ認証方法。

【請求項２２】

前記送信予告情報生成ステップにおいて、分割前の前記メッセージに対応する前記送信予告情報を生成し、

前記メッセージ認証ステップの前に、前記メッセージの全ての前記データブロックを結合して前記メッセージを復元するステップをさらに含み、

前記メッセージ認証ステップにおいて、復元された前記メッセージを前記送信予告情報を用いて認証することを特徴とする、請求項２０に記載のメッセージ認証方法。

【請求項２３】

前記送信予告情報生成ステップの前に、公開された所定の一方向性関数を任意の前記データブロックに適用して生成された認証情報を、別の前記データブロックに付加し、前記認証情報が付加されたデータブロックに前記一方向性関数を適用することを繰り返して、前記認証情報を前記各データブロックに付加する認証情報付加ステップをさらに含むことを特徴とする、請求項２０に記載のメッセージ認証方法。

【請求項２４】

前記一方向性関数は、ハッシュ関数であることを特徴とする、請求項２３に記載のメッセージ認証方法。

【請求項２５】
前記送信予告情報生成ステップにおいて、最後に生成された前記認証情報である第１認証情報に対応する前記送信予告情報を生成し、
前記メッセージ送信ステップの前に、
前記第１認証情報及び前記送信予告情報生成鍵を前記メッセージ受信装置に対して送信するステップと、
前記送信予告情報及び前記認証子生成鍵を用いて前記第１認証情報の認証を行う認証情報認証ステップと、
をさらに含むことを特徴とする、請求項２３または２４に記載のメッセージ認証方法。
【請求項２６】
前記メッセージ送信ステップにおいて、前記認証情報を生成するのに用いられたのと逆の順序で、前記データブロックを送信し、
前記メッセージ認証ステップにおいて、前記データブロックの直前に受信したデータブロックに含まれる前記認証情報を用いて前記データブロックの認証を行うことを特徴とする、請求項２３～２５のいずれかに記載のメッセージ認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メッセージ認証システム及びメッセージ認証方法に関する。
【背景技術】
【０００２】
近年、小型の無線通信装置を内蔵した多数のセンサを用いて、ワイヤレスで情報を収集・管理するセンサネットワークシステムが開発されており、例えば、工場等の施設内の設備管理、ビルや住宅の防犯・防災設備の管理、環境の観測等、様々な分野への適用が提案されている。センサネットワークシステムは、システム全体を管理・制御するサーバと、低コストで開発される多数のセンサノードとからなり、サーバは、センサノードにメッセージを送信し、ノードは、受信したメッセージがサーバから送信されたものであることを認証する。このようなセンサネットワークシステムにおいては、サーバ及びノード間の通信は、複数のノードがデータを中継して伝送するマルチホップ通信形態をとるのが一般的である。
【０００３】
センサネットワークシステムにおけるノードは、低コスト化を要求されるため、高い処理能力を有するＣＰＵ等を搭載した装置や、高タンパ性の装置が用いられるとは限らない。したがって、メッセージ認証において公開鍵暗号系の方法を採用するには、ＣＰＵにかかる処理負荷が大きくなりすぎる可能性があり、処理負荷の小さい共通鍵暗号系を用いる手法が望ましい。例えば、サーバと全ノードに全デバイス共通鍵を持たせてサーバからのメッセージを認証する方式がそれに該当する。しかし、ノードの高タンパ性が保証されない状況では、ノードに記憶させた全デバイス共通鍵が漏洩する可能性がある。このため、認証に成功したメッセージであっても、攻撃者がメッセージ挿入攻撃により投入した不正なメッセージ（Ｎｏｄｅ　Ｃｏｍｐｒｏｍｉｓｅ　Ａｔｔａｃｋ）である可能性がある。あるいは、マルチホップ通信の中継途中で不正なルータノードによって改ざんされたメッセージ（Ｎｏｄｅ　Ｒｅｐｌｉｃａｔｉｏｎ　Ａｔｔａｃｋ）である可能性もある。
【０００４】
特許文献１及び非特許文献１には、上述したような状況下でサーバからのブロードキャストメッセージを認証するにあたり、攻撃者のサーバへのなりすまし攻撃に耐性を持たせた方法が開示されている。
【０００５】
例えば、特許文献１に記載の方法によると、サーバがブロードキャストしたデータをノードが受信し、ノードは、ブロードキャストデータに対する受信確認をサーバに返信する。サーバは、受信確認が返信されたことを確認できた後に、まだネットワーク内に公開し

ていない認証鍵をノードに公開し、ノードは、公開された鍵が確かにサーバの認証鍵であることを確認することで、既に受信しているデータをサーバからの正しいデータであると認証することができる。

【０００６】

また、非特許文献１に記載の方法によると、サーバはデータをブロードキャストし、ノードは、ブロードキャストされたデータをバッファに格納する。サーバは、所定のタイムスケジュールに従ってノードに鍵を開示し、ノードは開示された鍵を認証し、鍵が正当であればその鍵を用いてバッファに格納したデータを認証する。データの認証に失敗した場合、データは異常に長く遅延して伝送されており、途中で改ざんされた可能性があることを検知することができる。

【０００７】

【特許文献１】特開２００６－１５７８５６号公報

【非特許文献１】Ａｄｒｉａｎ　Ｐｅｒｒｉｇ，Ｊ．Ｄ．　Ｔｙｇｅｒ著，溝口文雄監訳「ワイヤード／ワイヤレスネットワークにおけるブロードキャスト通信のセキュリティ」，共立出版　ｐｐ．１７２－１７７

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかし、特許文献１及び非特許文献１に記載されたような従来の方法では、認証鍵がノードに公開されるまで、ノードは受信したブロードキャストデータを認証することができない。その結果、ノードは、認証鍵が公開されるまで受信したメッセージを保持しておかなければならない。この問題は、ノードがメッセージを認証するまでの間のメモリの利用可能領域を狭めることにつながり、小容量のメモリしか搭載しないノードにとっては大きな負担となることがある。

【０００９】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、サーバ（メッセージ送信装置）が認証鍵を公開するまでの間にノード（メッセージ受信装置）が保持しなければならないデータ容量を減少させることが可能な、新規かつ改良されたメッセージ認証システム及びメッセージ認証方法を提供することにある。

【課題を解決するための手段】

【００１０】

上記課題を解決するために、本発明のある観点によれば、マルチホップ型ネットワークにおいて、メッセージを送信するメッセージ送信装置と、送信されたメッセージの認証を行うメッセージ受信装置とを備えるメッセージ認証システムが提供される。上記メッセージ送信装置は、メッセージの認証に用いられる２以上の認証子生成鍵を含む認証子生成鍵鎖列を管理する認証子生成鍵管理部と、認証子生成鍵を用いて、メッセージの正当性を証明するための第１認証子及び第１認証子の正当性を証明するための第２認証子からなる送信予告情報を生成する送信予告情報生成部と、送信予告情報を前記メッセージ受信装置に送信し、送信予告情報に対応してメッセージ受信装置から送信される受信証明情報を認証した後で、メッセージと認証子生成鍵とを送信する送信部とを含む。また、上記メッセージ受信装置は、送信予告情報の受信を証明する受信証明情報を生成する受信証明情報生成部と、第２認証子とメッセージ送信装置から送信された認証子生成鍵とを用いて第１認証子の認証を行う第１認証子認証部と、認証された第１認証子と認証子生成鍵とを用いて、メッセージ送信装置から受信したメッセージの認証を行うメッセージ認証部とを含む。

【００１１】

また、認証子生成鍵管理部は、任意の値に対し、公開された一方向性関数を実行する回数を順次増加させることにより各認証子生成鍵を生成し、生成された順と逆の順序で各認証子生成鍵をメッセージ受信装置に対して公開するようにしてもよい。

【００１２】

また、送信予告情報生成部は、未公開の認証子生成鍵、または未公開の認証子生成鍵に

公開された所定の一方向性関数を適用して生成された値のいずれかを用いて、第１認証子を生成するようにしてもよい。

【００１３】

また、送信予告情報生成部は、未公開の認証子生成鍵、または未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかと、第１認証子とを用いて、第２認証子を生成するようにしてもよい。

【００１４】

メッセージ受信装置は、受信した認証子生成鍵が未公開であるか否かを検証し、認証子生成鍵が未公開であれば、当該認証子生成鍵を用いて第１認証子の認証を行うようにしてもよい。

【００１５】

また、メッセージ受信装置は、メッセージ送信装置から認証子生成鍵が送信されるまで、受信した送信予告情報を受信順に保持する送信予告情報保持部をさらに含むようにしてもよい。さらに、第１認証子認証部は、送信予告情報保持部に保持されている送信予告情報に含まれる第１認証子を受信順に認証し、認証される場合、送信予告情報保持部に保持された他の前記送信予告情報を破棄し、認証されない場合、当該送信予告情報を破棄するようにしてもよい。

【００１６】

また、メッセージ送信装置は、メッセージを２以上のデータブロックに分割して送信するようにしてもよい。

【００１７】

また、送信予告情報生成部は、各データブロックに対応する送信予告情報を生成してもよい。さらに、メッセージ認証部は、各データブロックに対応する送信予告情報を用いて各データブロックを認証するようにしてもよい。

【００１８】

また、送信予告情報生成部は、分割前のメッセージに対応する送信予告情報を生成するようにしてもよい。さらに、メッセージ認証部は、メッセージの全てのデータブロックを結合してメッセージを復元し、復元されたメッセージを送信予告情報を用いて認証するようにしてもよい。

【００１９】

また、メッセージ送信装置は、認証情報を各データブロックに付加する認証情報付加部をさらに含むようにしてもよい。認証情報付加部は、公開された所定の一方向性関数を任意のデータブロックに適用して認証情報を生成し、生成された認証情報を他のデータブロックに付加し、さらに、認証情報が付加されたデータブロックに一方向性関数を適用することを繰り返して認証情報を生成するようにしてもよい。

【００２０】

また、一方向性関数は、ハッシュ関数であってもよい。

【００２１】

また、送信予告情報生成部は、最後に生成された認証情報である第１認証情報に対応する送信予告情報を生成するようにしてもよい。送信部は、データブロックの送信前に第１認証情報と認証子生成鍵とをメッセージ受信装置に対して送信し、メッセージ受信装置から第１認証情報が認証された旨の通知を受け取った後、データブロックを送信するようにしてもよい。メッセージ受信装置は、送信予告情報及び認証子生成鍵を用いて第１認証情報の認証を行う認証情報認証部をさらに含むようにしてもよい。

【００２２】

また、送信部は、認証情報を生成するのに用いられたのと逆の順序で、データブロックを送信し、メッセージ認証部は、データブロックの直前に受信したデータブロックに含まれる認証情報を用いてデータブロックの認証を行うようにしてもよい。

【００２３】

また、上記課題を解決するために、本発明の別の観点によれば、マルチホップ型ネット

ワークによってメッセージ送信装置から送信されたメッセージをメッセージ受信装置において認証するメッセージ認証方法が提供される。このメッセージ認証方法は、メッセージ送信装置からメッセージ受信装置に送信するメッセージを生成するメッセージ生成ステップと、メッセージ送信装置において、メッセージの認証に用いられる２以上の認証子生成鍵を含む認証子生成鍵鎖列を生成する認証子生成鍵生成ステップと、メッセージ送信装置において、認証子生成鍵を用いてメッセージの正当性を証明するための第１認証子及び第１認証子の正当性を証明するための第２認証子を含む送信予告情報を生成する送信予告情報生成ステップと、メッセージ送信装置からメッセージ受信装置に対し、送信予告情報を送信する送信予告情報送信ステップと、メッセージ受信装置において送信予告情報を受信したことを証明する受信証明情報を生成する受信証明情報生成ステップと、メッセージ受信装置から送信される受信証明情報をメッセージ送信装置が認証する受信証明情報認証ステップと、メッセージ送信装置からメッセージ受信装置に対し、認証子生成鍵を送信する認証子生成鍵送信ステップと、メッセージ送信装置からメッセージ受信装置に対し、メッセージを送信するメッセージ送信ステップと、第２認証子とメッセージ送信装置から送信された認証子生成鍵とを用いて、メッセージ受信装置が第１認証子の認証を行う第１認証子認証ステップと、認証された第１認証子と認証子生成鍵とを用いてメッセージの認証を行うメッセージ認証ステップと、を含む。

【００２４】

また、送信予告情報生成ステップは、公開された任意の値に対し、公開された一方向性関数を実行する回数を順次増加させることにより各認証子生成鍵を生成し、認証子生成鍵鎖列に含まれる各認証子生成鍵は、生成順と逆の順序でメッセージ受信装置に対して公開されるようにしてもよい。

【００２５】

また、送信予告情報生成ステップにおいて、未公開の認証子生成鍵、または未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかを用いて、第１認証子を生成するようにしてもよい。

【００２６】

また、送信予告情報生成ステップにおいて、未公開の認証子生成鍵、または未公開の認証子生成鍵に公開された所定の一方向性関数を適用して生成された値のいずれかと、第１認証子とを用いて、第２認証子を生成するようにしてもよい。

【００２７】

また、第１認証子認証ステップの前に、メッセージ受信装置は、受信した前記認証子生成鍵が未公開であるか否かを検証し、認証子生成鍵が未公開であれば、当該認証子生成鍵を用いて第１認証子の認証を行うようにしてもよい。

【００２８】

また、メッセージ受信装置は、メッセージ送信装置から認証子生成鍵が送信されるまで、受信した送信予告情報を受信順に保持し、第１認証子認証ステップにおいて、保持されている送信予告情報に含まれる第１認証子を受信順に認証し、認証される場合、他の送信予告情報を破棄し、認証されない場合、当該送信予告情報を破棄するようにしてもよい。

【００２９】

また、メッセージ生成ステップにおいて、メッセージを２以上のデータブロックに分割して生成するようにしてもよい。

【００３０】

また、送信予告情報生成ステップにおいて、各データブロックに対応する送信予告情報を生成し、メッセージ認証ステップにおいて、各データブロックに対応する送信予告情報を用いて各データブロックを認証するようにしてもよい。

【００３１】

また、送信予告情報生成ステップにおいて、分割前のメッセージに対応する送信予告情報を生成し、メッセージ認証ステップの前に、メッセージの全てのデータブロックを結合してメッセージを復元するステップをさらに含み、メッセージ認証ステップにおいて、復

元されたメッセージを送信予告情報を用いて認証するようにしてもよい。

【００３２】

また、送信予告情報生成ステップの前に、公開された所定の一方向性関数を任意のデータブロックに適用して生成された認証情報を、別のデータブロックに付加し、認証情報が付加されたデータブロックに一方向性関数を適用することを繰り返して、認証情報を各データブロックに付加する認証情報付加ステップをさらに含むようにしてもよい。

【００３３】

また、一方向性関数は、ハッシュ関数であってもよい。

【００３４】

また、送信予告情報生成ステップにおいて、最後に生成された認証情報である第１認証情報に対応する送信予告情報を生成し、メッセージ送信ステップの前に、第１認証情報及び送信予告情報生成鍵をメッセージ受信装置に対して送信するステップと、送信予告情報及び認証子生成鍵を用いて第１認証情報の認証を行う認証情報認証ステップと、をさらに含むようにしてもよい。

【００３５】

また、メッセージ送信ステップにおいて、認証情報を生成するのに用いられたのと逆の順序でデータブロックを送信し、メッセージ認証ステップにおいて、データブロックの直前に受信したデータブロックに含まれる認証情報を用いてデータブロックの認証を行うようにしてもよい。

【発明の効果】

【００３６】

以上説明したように本発明によれば、サーバ（メッセージ送信装置）が認証鍵を公開するまでの間、ノード（メッセージ受信装置）が保持しなければならないデータ容量を減少させることができる。

【発明を実施するための最良の形態】

【００３７】

以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【００３８】

（従来の方式における問題点）

従来のセンサネットワークにおいては、サーバから認証鍵が公開されるまでノード側で受信したデータを保持しなければならず、小容量のメモリしか搭載しないノードにとっては大きな負担となっていた。かかる問題を解決するために、従来、サーバが認証させたいメッセージの送信予告情報を先に送信し、その送信予告情報に対する受信確認を行った後認証鍵とメッセージを送信する方式が考案されている。

【００３９】

図２９は、このような従来のメッセージ認証方式の処理の流れを示すシーケンス図である。図２９を参照して、サーバ（メッセージ送信装置）１１からノード（メッセージ受信装置）１２にメッセージＭを送信する場合の処理について説明する。まず、サーバ１１は、ノード１２に対して送信予告情報を送信する（ステップＳ２０）。ここで、送信予告情報１３は、メッセージＭに対し認証子生成鍵Ｋを用いて生成したメッセージ認証子（ＭＡＣ；Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅｓ）であって、ＭＡＣ（Ｋ，Ｍ）と表される。ノード１２は、送信予告情報ＭＡＣ（Ｋ，Ｍ）を受信し、受信確認をサーバ１１に返信する（ステップＳ２１）。サーバ１１は、受信確認の検証を行い、検証に成功したら（ステップＳ２２）、メッセージＭと認証子生成鍵Ｋとをノード１２に送信する（ステップＳ２３）。ノード１２は、受信した認証子生成鍵Ｋの検証を行い、サーバ１１から送信された正当な鍵であることを認証したら、認証子生成鍵Ｋと送信予告情報ＭＡＣ（Ｋ，Ｍ）とを用いてメッセージＭの認証を行う（ステップＳ２４）。かかる方法によると、ノードは、認証子生成鍵が公開されるまでの間、送信予告情報を保持すればよ

く、メッセージそのものを保持する必要がないので、ノードが保持しなければならないデータ容量を減少させることができる。

【００４０】

しかし、このような従来の方式では、ノードが複数のメッセージの送信予告情報の受信を許容する場合に、不正な中継ノードによって送信された不正なメッセージを誤って認証してしまうことがあるという問題があった。図３０は、このような従来のメッセージ認証方式の処理における攻撃例を示すシーケンス図である。図３０を参照して、不正な中継ノード３３（以下、不正ノード３３と呼ぶ）が、不正なメッセージＭ’をノード３２に送信しようとする場合について説明する。

【００４１】

まず、不正ノード３３は、不正な認証子生成鍵Ｋ’を用いて生成した送信予告情報ＭＡＣ（Ｋ’，Ｍ’）をノード３２に送信し（ステップＳ４０）、ノード３２は、受信確認を返信する（ステップＳ４１）。次に、サーバ３１が、正当なメッセージの送信予告情報ＭＡＣ（Ｋ，Ｍ）を不正ノード３３を経由してノード３２に送信する（ステップＳ４２）。ノード３２は、サーバ３１に受信確認を返信する（ステップＳ４３）。サーバ３１は、受信確認の検証を行い（ステップＳ４４）、正当な認証子生成鍵Ｋとメッセージ Ｍとを送信する（ステップＳ４５）。不正ノード３３は、認証子生成鍵Ｋ及びメッセージＭの中継時に、正当な認証子生成鍵Ｋを用いて不正なメッセージＭ’の送信予告情報ＭＡＣ（Ｋ，Ｍ’）を生成し、ノード３２に送信する（ステップＳ４６）。その後、ノード３２から受信確認が送信されたら（ステップＳ４７）、正当な認証子生成鍵Ｋと不正なメッセージＭ’をノード３２に送信する（ステップＳ４８）。

【００４２】

このような場合、ノード３２は、受信済みのどの送信予告情報でメッセージを検証すればよいかが分からないため、不正ノード３３から送信された送信予告情報ＭＡＣ（Ｋ，Ｍ’）によって不正なメッセージＭ’を正当なメッセージとして認証してしまう可能性があった。

【００４３】

そこで、本発明では、メッセージ送信装置（サーバ）が認証させたいメッセージの送信予告情報とメッセージの送信予告情報の正当性を証明するための認証子を先に送信し、その後、認証子生成鍵とメッセージを送信することで、メッセージ受信装置（ノード）が複数のメッセージ送信予告情報の受信を許容する場合であっても、不正なメッセージ送信予告情報を排除できるようにする。

【００４４】

（第１の実施形態）

まず、図１を参照して、本発明の第１の実施形態にかかるメッセージ認証システムについて説明する。図１は、本実施形態にかかるメッセージ認証システム１００の概略構成を示すブロック図である。図１に示すように、本実施形態にかかるメッセージ認証システムは、１つのメッセージ送信装置（サーバ）１１０及び複数のメッセージ受信装置（ノード）１２０－１～１２０－５（以下、メッセージ受信装置１２０と総称する）により構成される。メッセージ受信装置１２０は、例えば、小型の無線通信装置を内蔵した装置であって、メッセージ送信装置１１０と各メッセージ受信装置１２０とは、互いに無線通信によりデータの送受信を行う。また、メッセージ送信装置１１０と各メッセージ受信装置１２０との間の通信は、マルチホップ通信により行われる。例えば、メッセージ送信装置１１０からメッセージ受信装置１２０－４に対してデータを送信する場合、データは、メッセージ受信装置１２０－１及び１２０－２を順に経由してメッセージ受信装置１２０－４に送信される。

【００４５】

本実施形態にかかるメッセージ認証システム１００は、メッセージ送信装置１１０が、メッセージに対して生成した第１の認証子とその認証子の正当性を証明するための第２の認証子とをメッセージ受信装置１２０に送信し、上記２つの認証子がメッセージ受信装置

１２０に到達したことを確認した後、認証子生成鍵とメッセージとを送信することを特徴とする。

【００４６】

（メッセージ送信装置１１０）

まず、図２を参照して、本実施形態にかかるメッセージ認証システム１００におけるメッセージ送信装置（サーバ）１１０について説明する。図２は、本実施形態にかかるメッセージ送信装置（サーバ）１１０の概略構成を示すブロック図である。図２に示すように、メッセージ送信装置１１０は、メッセージ生成部１１１、認証子生成鍵管理部１１２、メッセージ保持部１１３、送信予告情報生成部１１４、送信情報生成部１１５、受信証明検証部１１６、受信部１１７及び送信部１１８により構成される。以下、メッセージ送信装置１１０の各部について説明する。

【００４７】

（メッセージ生成部１１１）

メッセージ生成部１１１は、メッセージ送信装置（サーバ）１１０がメッセージ受信装置（ノード）１２０に対して送信するメッセージを生成するための機能部である。メッセージ生成部１１１は、生成したメッセージＭを１以上のデータブロックM_j（$1 \leqq j \leqq n$，$n \geqq 1$）に分割し、分割された各データブロックM_jを送信予告情報生成部１１４に渡す。

【００４８】

（認証子生成鍵管理部１１２）

認証子生成鍵管理部１１２は、メッセージの認証子生成に用いられる認証子生成鍵鎖列K_i（$0 \leqq i \leqq m$，$m \geqq 1$）を管理するための機能部である。図４は、認証子生成鍵管理部１１２によって管理される認証子生成鍵鎖列を説明するための説明図である。図４に示すように、認証子生成鍵鎖列は、例えば、メッセージ送信装置１１０内で決定された任意の初期値K_mと、K_mに所定の一方向性関数Ｆ（）を複数回適用したときの各出力値K_{m-1}，K_{m-2}，…，K_1，K_0（$K_i = F(K_{i+1})$）で構成される。ここで、一方向性関数Ｆ（）は、メッセージ送信装置１１０及びメッセージ受信装置１２０の双方において公開された関数である。また、メッセージ送信装置１１０とメッセージ受信装置１２０とは、初期状態において認証子生成鍵K_0を安全に共有するものとする。また、生成された認証子生成鍵鎖列の各認証子生成鍵は、生成されたときと逆の順番（$K_0 \rightarrow K_1 \rightarrow \cdots$）で利用される。

【００４９】

図４に示すように、認証子生成鍵鎖列に含まれる認証子生成鍵は、ネットワークに公開済みであるか未公開であるかの区別がされている。また、認証子生成鍵鎖列の未公開の認証子生成鍵のうち、次に公開される認証子生成鍵をアクティブ鍵K_a（$0 \leqq a \leqq m$，$m \geqq 1$）として設定する。上述したとおり、認証子生成鍵鎖列の各認証子生成鍵は、$K_0 \rightarrow K_1 \rightarrow \cdots$の順に利用され公開されることから、$K_0$，$K_1$，…，$K_{a-1}$は、ネットワークに公開済みであって、$K_a$，…，$K_{m-1}$，$K_m$は、ネットワークに未公開の鍵である。

【００５０】

認証子生成鍵管理部１１２は、送信予告情報生成部１１４からの要求に応じて、現在のアクティブ鍵K_aを送信予告情報生成部１１４に与える。また、受信証明検証部１１６から受信証明検証終了メッセージが送信されて、受信証明情報の検証が終了したことが通知されると、現在のアクティブ鍵K_aを送信情報生成部１１５に与え、ネットワークに公開する。これにより、現在のアクティブ鍵K_aは公開された状態となるため、認証子生成鍵管理部１１２は、ａ＝ａ＋１とし、アクティブ鍵K_aを、次に公開される認証子生成鍵K_{a+1}に更新する。

【００５１】

認証子生成鍵管理部１１２は、生成された認証子生成鍵鎖列全体を保持するようにしてもよいし、あるいは、初期値K_mのみを保持し、要求がある毎に一方向性関数Ｆを所定の回数適用することによって、各認証子生成鍵を生成するようにしてもよい。

【００５２】
（メッセージ保持部１１３）
メッセージ保持部１１３は、メッセージ受信装置１２０に送信するメッセージのデータブロックM_jを保持するための記憶部である。メッセージ保持部１１３は、送信予告情報生成部１１４から与えられたデータブロックM_jを保持し、受信証明検証部１１６から受信証明検証終了メッセージが送信されて受信証明情報の検証が終了したことが通知されると、保持しているデータブロックM_jを送信情報生成部１１５に与える。
【００５３】
（送信予告情報生成部１１４）
送信予告情報生成部１１４は、任意のデータに対する第１認証子と第２認証子とからなる送信予告情報を生成するための機能部である。送信予告情報生成部１１４は、メッセージ生成部１１１によって生成されるデータブロックM_jに対し、認証子生成鍵管理部１１２より与えられる認証子生成鍵または認証子生成鍵から派生して生成される派生情報を用いて、第１認証子を生成する。さらに、生成した第１認証子に対し、認証子生成鍵管理部１１２より与えられる認証子生成鍵またはその派生情報を用いて、第２認証子を生成する。第１認証子は、データブロックM_jの正当性を証明するための情報であり、第２認証子は、第１認証子の正当性を証明するための情報である。
【００５４】
第１認証子及び第２認証子を生成するのに用いられる認証子生成アルゴリズムとしては、ＨＭＡＣ（ＨＭＡＣ；Keyed-Hashing for Message Authentication Code）やＣＢＣ－ＭＡＣ（ＣＢＣ－ＭＡＣ；Cipher Block Chaining-Message Authentication Code）等であってもよいし、上記以外のアルゴリズムであってもよく、特に限定するものではない。
【００５５】
本実施形態においては、認証子生成鍵管理部１１２より認証子生成鍵K_aが与えられる場合、第１認証子を生成するのに用いられる認証子生成鍵を$K_a' = G(K_a)$とし、第２認証子を生成するのに用いられる認証子生成鍵をK_aとするが、特に限定するものではなく、上記以外の認証子生成鍵を用いてもよい。また、第１認証子と第２認証子とは生成に用いられる認証子生成鍵が異なるものとするが、これについても特に限定するものではなく、同一の認証子生成鍵が用いられてもよい。ここで、Ｇ（）は、一方向性関数を表し、メッセージ送信装置１１０及びメッセージ受信装置１２０において公開された関数であるものとする。
【００５６】
また、送信予告情報生成部１１４は、生成した第１認証子と第２認証子とを送信予告情報として送信情報生成部１１５に与える。また、メッセージ生成部より与えられたデータブロックM_jをメッセージ保持部１１３に与える。
【００５７】
（送信情報生成部１１５）
送信情報生成部１１５は、各部からメッセージ受信装置１２０に対して送信するデータを収集し、収集したデータを送信するための送信情報を生成するための機能部である。送信情報生成部１１５は、送信予告情報生成部１１４から与えられる送信予告情報（第１認証子及び第２認証子）、メッセージ保持部から与えられるデータブロックM_{j-1}、認証子生成鍵管理部１１２から与えられるK_{a-1}のうちの１つまたは複数の情報からなる送信情報を生成し、生成した送信情報を受信証明検証部１１６と送信部１１８とに与える。
【００５８】
（受信証明検証部１１６）
受信証明検証部１１６は、メッセージ受信装置１２０から受信した受信証明情報を用いて、送信した送信情報が対象となるメッセージ受信装置１２０によって受信されたか否かを検証するための機能部である。受信証明検証部１１６は、受信部１１７より与えられる受信証明情報を検証することにより、対象とする全メッセージ受信装置１２０に送信情報

が偽りなく届いたか、または、対象とするメッセージ受信装置１２０のうちの特定のメッセージ受信装置には送信情報が偽りなく届けられなかったかを確認する。確認終了後、受信証明検証部１１６は、認証子生成鍵管理部１１２とメッセージ保持部１１３とに対して、受信証明検証終了メッセージを送信し、受信証明情報の検証が終了したことを通知する。

【００５９】

特定のメッセージ受信装置に送信情報が偽りなく届けられなかったことが確認された場合、そのメッセージ受信装置が故障、盗難あるいは攻撃等にあっている可能性があるため、後にネットワークから離脱させるようにしてもよい。あるいは、送信情報生成部１１５から与えられた送信情報を送信部１１８に与えて、該当するメッセージ受信装置に対して送信情報を再送するようにしてもよい。

【００６０】

送信情報が受信されたか否かを検証する検証方法としては、例えば、次のような方法を用いてもよい。受信証明検証部１１６と、メッセージの送信対象であるメッセージ受信装置１２０とは、各々１対の共有鍵を共有する。メッセージ受信装置１２０は、メッセージ送信装置１１０から受信した送信情報に対して、上述の共有鍵を用いて生成した認証子（受信証明情報）を生成し、生成された認証子（受信証明情報）をメッセージ送信装置１１０へ送信する。メッセージ送信装置１１０は、受信証明検証部１１６において、共有鍵を用いてメッセージ受信装置１２０が受信した認証子（受信証明情報）を検証することで受信確認を得ることができる。なお、受信証明情報の検証方法は、上述した例に限られず、他の方法を用いてもよい。

【００６１】

（受信部１１７）

受信部１１７は、メッセージ受信装置１２０から送信されるデータを受信するための機能部である。受信部１１７は、メッセージ受信装置１２０から受信証明情報を受信し、受信証明検証部１１６に受信証明情報を与える。

【００６２】

（送信部１１８）

送信部１１８は、メッセージ受信装置１２０に対しデータを送信するための機能部である。送信部１１８は、送信情報生成部１１５より与えられた送信情報を、送信対象のメッセージ受信装置１２０に送信する。また、受信証明検証部１１６より指定される送信情報を、同じく受信証明検証部１１６によって指定されるメッセージ受信装置１２０へ再送信する。

【００６３】

以上、本実施形態にかかるメッセージ送信装置１１０の各部について説明した。なお、メッセージ生成部１１１、認証子生成鍵管理部１１２、送信予告情報生成部１１４、送信情報生成部１１５、受信証明検証部１１６、受信部１１７及び送信部１１８は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、メッセージ保持部１１３は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。

【００６４】

次に、図３を参照して、本実施形態にかかるメッセージ認証システム１００におけるメッセージ受信装置（ノード）１２０について説明する。図３は、本実施形態にかかるメッセージ受信装置（ノード）１２０の概略構成を示すブロック図である。図３に示すように、本実施形態にかかるメッセージ受信装置１２０は、受信部１２１、受信証明情報生成部１２２、認証子生成鍵検証部１２３、送信予告情報保持部１２４、第１認証子認証部１２５、メッセージ認証部１２６及び送信部１２７により構成される。以下、メッセージ受信装置１２０の各部について説明する。

【００６５】
（受信部１２１）
受信部１２１は、メッセージ送信装置１１０から送信された送信情報を受信するための機能部である。受信部１２１は、メッセージ送信装置１１０から各送信情報を受信し、受信証明情報生成部１２２に与える。
【００６６】
（受信証明情報生成部１２２）
受信証明情報生成部１２２は、受信部１２１より与えられた送信情報を確かに受信したことをメッセージ送信装置１１０に証明するための受信証明情報を生成するための機能部である。
【００６７】
送信情報を確かに受信したことをメッセージ送信装置１１０に対して証明する方法としては、例えば、次のような方法を用いてもよい。受信証明情報生成部１２２は、メッセージ送信装置１１０と１対の共有鍵の情報を共有する。受信証明情報生成部１２２は、受信部１２１より与えられた送信情報に対して、上述の共有鍵を用いて生成した認証子（受信証明情報）を生成し、生成された認証子（受信証明情報）を、送信部１２７を通してメッセージ送信装置１１０に返信する。メッセージ送信装置１１０は、例えば、受信証明検証部１１６において、共有鍵を用いてメッセージ受信装置１２０から送信された認証子（受信証明情報）を検証することで、受信確認を得ることができる。なお、受信証明の方法は、上述した例に限られず、他の方法を用いてもよいが、メッセージ送信装置１１０とメッセージ受信装置１２０との間で規定された共通の方法を用いる必要がある。
【００６８】
受信証明情報生成部１２２は、生成した受信証明情報を送信部１２７に与える。また、受信証明情報生成部１２２は、受信部１２１より与えられた第１認証子及び第２認証子を含む送信予告情報を送信予告情報保持部１２４へ渡す。また、受信部１２１より与えられたデータブロックM_jをメッセージ認証部１２６へ渡し、認証子生成鍵K_aを認証子生成鍵検証部へ渡す。
【００６９】
（認証子生成鍵検証部１２３）
認証子生成鍵検証部１２３は、メッセージ送信装置１１０から受信した認証子生成鍵K_aが正当な鍵であるか否かを検証するための機能部である。認証子生成鍵検証部１２３は、メッセージ送信装置１１０とメッセージ受信装置１２０とが初期状態において安全に共有する認証子生成鍵K_0を保持するものとする。また、過去に検証に成功した認証子生成鍵K_1，…，K_{a-1}を保持してもよい。認証子生成鍵検証部１２３は、受信証明情報生成部１２２より与えられた認証子生成鍵K_aに、システムで規定された一方向性関数Ｆ（）を適用した結果が、保持している認証子生成鍵K_aと一致するか否かを判定することにより、認証子生成鍵K_aが正当な鍵であるか否かを検証することができる。認証子生成鍵検証部１２３は、検証に成功した認証子生成鍵K_aを、最も新しくネットワークに公開された認証子生成鍵として新たに保持し、認証子生成鍵K_aを第１認証子認証部１２５に渡す。
【００７０】
（送信予告情報保持部１２４）
送信予告情報保持部１２４は、メッセージ送信装置１１０から受信した送信予告情報（第１認証子及び第２認証子）を保持するための記憶部である。送信予告情報保持部１２４は、受信証明情報生成部１２２より与えられた送信予告情報を、受信した順番を記憶しながら保持する。また、送信予告情報保持部１２４は、第１認証子認証部１２５からの要求に応じて、保持している送信予告情報を受信した順番に第１認証子認証部１２５に渡す。
【００７１】
（第１認証子認証部１２５）
第１認証子認証部１２５は、メッセージ送信装置１１０より与えられた送信予告情報に

含まれる第１認証子が正当なものであるか否かを検証するための機能部である。第１認証子認証部１２５は、送信予告情報保持部１２４よりデータブロックM_jに対する第１認証子及び第２認証子を受信した順番に与えられる。さらに、認証子生成鍵検証部１２３より認証子生成鍵K_aを与えられ、K_aと第２認証子とを用いて第１認証子が認証されるか否かを検証する。

【００７２】

具体的には、例えば、第１認証子認証部１２５は、認証子生成鍵K_aを用いて第１認証子に対する認証子を生成し、生成された認証子が、第２認証子と一致するか否かを判定することにより、第１認証子の認証を行う。第１認証子認証部１２５は、送信予告情報保持部１２４において保持されている送信予告情報の中で、一番初めに認証された第１認証子を、データブロックM_jの正当性を証明する正当な第１認証子であると認証し、その他の送信予告情報を破棄する。第１認証子認証部１２５は、正常に認証された第１認証子と認証子生成鍵K_aとをメッセージ認証部１２６に渡す。あるいは、認証子生成鍵K_aにシステムで規定された一方向性関数Ｇを適用した出力値K_a’を求め、認証子生成鍵K_aの代わりにメッセージ認証部１２６に渡すようにしてもよい。

【００７３】

（メッセージ認証部１２６）

メッセージ認証部１２６は、メッセージ送信装置１１０から受信したメッセージのデータブロックM_jが正当なメッセージであるかを認証するための機能部である。メッセージ認証部１２６は、受信証明情報生成部１２２よりデータブロックM_jを与えられ、第１認証子認証部１２５より与えられた認証子生成鍵K_aまたはK_a’と第１認証子とを用いてデータブロックM_jを認証する。第１認証子認証部１２５より認証子生成鍵K_aが与えられた場合は、システムで規定された一方向性関数ＧをK_aに適用し、K_a’を求める。メッセージ認証部１２６がM_jを認証する方法は、例えば、K_a’を用いてデータブロックM_jに対する認証子を生成し、生成された認証子が第１認証子と一致するか否かを判定する等の方法を用いて行ってもよい。一致した場合は、データブロックM_jは正当なメッセージであると認証される。一致しない場合は、不正なメッセージと判断され、メッセージ認証部１２６は、データブロックM_jを破棄する等してもよい。

【００７４】

（送信部１２７）

送信部１２７は、メッセージ送信装置１１０に対して情報を送信するための機能部である。送信部１２７は、受信証明情報生成部１２２より与えられる受信証明情報を、メッセージ送信装置１１０に返信する。

【００７５】

以上、本実施形態にかかるメッセージ受信装置１２０の各部について説明した。なお、受信部１２１、受信証明情報生成部１２２、認証子生成鍵検証部１２３、第１認証子認証部１２５、メッセージ認証部１２６及び送信部１２７は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、送信予告情報保持部１２４は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。

【００７６】

次に、図５～図１０に基づいて、本実施形態にかかるメッセージ認証システム１００により実行されるメッセージ認証処理の一例を説明する。ここで、図５及び６は、本実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。また、図７及び８は、本実施形態にかかるメッセージ認証処理のステップＳ１５５における状態を示した説明図である。同様に、図９は、ステップＳ１６３における状態を示した説明図であり、図１０は、送信情報再送時における状態を示した説明図である。

【００７７】

まず、ステップＳ１５０で、メッセージ送信装置１１０のメッセージ生成部１１１にお

いて、送信するメッセージMを生成する。次いで、ステップＳ１５１で、メッセージMを分割してｊ個のデータブロックM_j（１≦ｊ≦ｎ，ｎ≧１）を生成する。生成されたデータブロックM_jは、送信予告情報生成部１１４に渡される。

【００７８】

次いで、送信予告情報生成部１１４が第１認証子及び第２認証子（送信予告情報）を生成する。まず、ステップＳ１５２で、データブロックM_jに対する第１認証子（M_jの正当性を証明するための情報）を生成する。ここでは、ネットワークに未公開の現在のアクティブ鍵K_aに一方向性関数Gを適用して求められた値$K_a' = G(K_a)$を用いて第１認証子$MAC(K_a', M_j)$を生成する。ここで、関数Gは、システムで公開された関数であるものとする。

【００７９】

次いで、ステップＳ１５３で、第１認証子$MAC(K_a', M_j)$に対する第２認証子（第１認証子の正当性を証明するための情報）を生成する。ここでは、現在のアクティブ鍵K_aを用いて第２認証子$MAC(K_a, MAC(K_a', M_j))$を生成する。生成された第１認証子及び第２認証子は、送信情報生成部１１５に渡される。

【００８０】

次いで、ステップＳ１５４で、第１認証子$MAC(K_a', M_j)$、第２認証子$MAC(K_a, MAC(K_a', M_j))$を含む送信情報を生成する。また、送信情報には、メッセージ保持部１１３より与えられたデータブロックM_{j-1}，認証子生成鍵管理部１１２より与えられた認証子生成鍵K_{a-1}を含むようにしてもよい。ここで、データブロックM_{j-1}は、データブロックM_jの１つ前のデータブロックであって、既にメッセージ受信装置１２０に対して送信予告情報（第１認証子及び第２認証子）が送信され、メッセージ受信装置１２０において送信予告情報が受信されたことが確認されたデータブロックである。また、認証子生成鍵K_{a-1}は、現在のアクティブ鍵K_aの１つ前に公開される認証子生成鍵であって、データブロックM_{j-1}の送信予告情報の生成に用いられた認証子生成鍵である。

【００８１】

次いで、図７に示すように、ステップＳ１５５で、生成された送信情報１３０を送信部１１８を通してメッセージ受信装置１２０に送信し、メッセージ受信装置１２０は、図８に示すように、送信された送信情報１３０を受信する。その後、メッセージ送信装置１１０は、ステップＳ１５６で、送信した送信情報１３０を格納する。

【００８２】

次いで、ステップＳ１５７で、メッセージ受信装置１２０は、認証子生成鍵検証部１２３において、受信した認証子生成鍵K_{a-1}の認証を行う。例えば、認証子生成鍵K_{a-1}に、システムで規定された一方向性関数Ｆ（）を適用して、生成された値が、認証子生成鍵K_{a-1}の前に認証された認証子生成鍵K_{a-2}と一致するか否かを判定することにより、認証子生成鍵K_{a-1}の認証を行ってもよい。

【００８３】

認証子生成鍵K_{a-1}が正常に認証されたら、ステップＳ１５８で、認証子生成鍵K_{a-1}を格納する。

【００８４】

次いで、ステップＳ１５９で、メッセージ受信装置１２０において既に受信し、送信予告情報保持部１２４に保持されている送信予告情報に含まれる第１認証子の認証を行う。送信予告情報保持部１２４は、保持している送信予告情報を受信した順に第１認証子認証部１２５に与え、第１認証子認証部１２５において認証が行われる。送信予告情報保持部１２４には、既に、データブロックM_{j-1}に対する送信予告情報が格納されている。例えば、第１認証子認証部１２５は、認証子生成鍵K_{a-1}を用いて第１認証子に対する認証子を生成し、生成された認証子が第２認証子と一致するか否かを判定することにより、第１認証子を認証する。

【００８５】

認証が正常に行われなかった場合は、ステップＳ１６０に進み、その送信予告情報を破棄する。認証が正常に行われた場合は、ステップＳ１６１に進み、認証された送信予告情報以外の送信予告情報を破棄する。

【００８６】

次いで、ステップＳ１６２で、メッセージ認証部１２６においてデータブロックM_{j-1}の認証を行う。メッセージ認証部１２６は、例えば、ステップＳ１５７で認証された認証子生成鍵K_{a-1}にシステムで規定された一方向性関数Ｇを適用して求めた値K_{a-1}’を用いて、M_{j-1}に対する認証子を生成し、生成された値がステップＳ１５９で認証された第１認証子と一致するかを判定することにより、データブロックM_{j-1}の認証を行う。

【００８７】

次いで、図９に示すように、ステップＳ１６３において、ステップＳ１５５で受信した送信予告情報に対する受信証明情報１３１を受信証明情報生成部１２２が生成し、送信部１２７を通してメッセージ送信装置１１０に送信する。その後、ステップＳ１６４で、送信予告情報を受信順に送信予告情報保持部１２４に格納する。

【００８８】

ステップＳ１６５で、メッセージ送信装置１１０は、受信証明検証部１１６においてメッセージ受信装置１２０より受信した受信証明情報１３１の検証を行う。検証により、受信が確認された場合は、ステップＳ１６６に進み、データブロックM_jを送信することが決定される。次いで、ステップＳ１６７で、送信予告情報の生成に用いられた認証子生成鍵K_aをネットワークに公開することが決定される。さらに、ステップＳ１６８で、アクティブ鍵K_aをK_{a+1}に更新する。

【００８９】

ステップＳ１６５において受信証明情報１３１を検証した結果、受信が確認できなかった場合は、図１０に示すように、送信情報１３０をメッセージ受信装置１２０に対して再送信するようにしてもよい。

【００９０】

以上、本実施形態にかかるメッセージ認証システム１００により実行されるメッセージ認証処理の一例を説明した。

【００９１】

本実施形態の構成によれば、メッセージ送信装置は、メッセージのデータブロックに対して生成した第１認証子と第２認証子とをメッセージ受信装置に送信し、かかる２つの認証子がメッセージ受信装置に到達したことを確認した後で、認証子生成鍵とデータブロックとを送信する。これにより、メッセージ受信装置が複数の送信予告情報（第１認証子及び第２認証子）の受信を許容する場合であっても、不正な送信予告情報を排除することができるようになる。

【００９２】

図１１を参照して、本実施形態にかかるメッセージ認証システム１００による効果を説明する。図１１は、本実施形態にかかるメッセージ認証システム１００の効果を説明するためのシーケンス図である。

【００９３】

図１１において、ＭＡＣ（Ｘ，Ｙ）は、データＹに対して鍵Ｘを用いて生成した認証子を、Ｋ１は、サーバ（メッセージ送信装置）１１０が保持する正当な認証子生成鍵を、Ｋ１’は、Ｋ１に一方向性関数Ｇを適用した値（Ｋ１’＝Ｇ（Ｋ１））を、Ｍ１は、サーバが生成した正当なメッセージを、Ｋ’とＫ”は、不正ノード１９０が生成した意味を持たない鍵を、Ｍ１’は、不正ノード１９０が生成した不正なメッセージを、それぞれ示す。ノード（メッセージ受信装置）１２０が、複数のメッセージの送信予告情報の受信を許容する場合の攻撃モデルとして、以下の２つのモデルを想定する。

【００９４】

（攻撃モデルＡ）

不正ノード（攻撃者）１９０は、認証子生成鍵Ｋ１が公開される前に、不正な鍵Ｋ”を用いて不正なメッセージＭ１’に対して作成した、不正な送信予告情報（第１認証子ＭＡＣ（Ｋ”，Ｍ１’）及び第２認証子（ＭＡＣ（Ｋ’，ＭＡＣ（Ｋ”，Ｍ１’））をノード１２０に送信する。ノード１２０は、受信確認を送信し（ステップＳ１８１）、認証子生成鍵Ｋ１が公開されるまで、送信された送信予告情報を保持する。

【００９５】

（攻撃モデルＢ）

サーバ１１０から正当な認証子生成鍵Ｋ１と正当なメッセージＭ１とが送信された後、不正ノード（攻撃者）１９０は、公開された正当な認証子生成鍵Ｋ１を用いて、不正なデータブロックＭ１’に対する送信予告情報（第１認証子ＭＡＣ（Ｋ１’，Ｍ１’）及び第２認証子（ＭＡＣ（Ｋ１，ＭＡＣ（Ｋ１’，Ｍ１’）をノード１２０に送信する。

【００９６】

攻撃モデルＡの場合、ノード（メッセージ受信装置）１２０は、公開された正当な鍵Ｋ１を用いて、第１認証子を認証することができない。よって、攻撃モデルＡの場合、ノードにおいて、攻撃者は、不正なメッセージを正当なメッセージとして認証させることはできない。

【００９７】

攻撃モデルＢの場合、ノード（メッセージ受信装置）１２０は、公開された正当な認証子生成鍵Ｋ１を用いて、不正な第１認証子を認証してしまう。しかし、不正な第１認証子の認証を行う前に、正当な送信予告情報の認証を行うため、ここで、正当な送信予告情報は認証される。もしここで、正当な送信予告情報が認証されない場合、認証子生成鍵Ｋ１はネットワークに公開されていないことになるので、攻撃者１９０は、正当な認証子生成鍵Ｋ１を入手することができない。従って、送信予告情報は、正当な送信予告情報の認証後、受信の順番により破棄されることとなり、攻撃者１９０は、不正なメッセージを正当なメッセージとして認証させることはできない。

【００９８】

以上より、本実施形態にかかるメッセージ認証情報によると、メッセージ受信装置が複数のメッセージの送信予告情報を許容する場合であっても、不正なメッセージの送信予告情報を排除することができ、その結果、正当なメッセージのみを認証することができる。

【００９９】

（第２の実施形態）

次に、図１２及び１３を参照して、本発明の第２の実施形態にかかるメッセージ認証システムについて説明する。本実施形態にかかるメッセージ認証システムは、メッセージ送信装置が、複数のデータブロックM_jに分割する前のメッセージＭ全体に対して第１認証子及び第２認証子を生成し、２つの認証子がメッセージ受信装置に到達したことを確認した後で、認証子生成鍵を公開し、その後データブロックM_1、M_2、…、M_nを順次送信するようにしたことを特徴とするものである。

【０１００】

（メッセージ送信装置２１０）

まず、図１２を参照して、本実施形態にかかるメッセージ認証システムのメッセージ送信装置２１０について説明する。図１２は、本実施形態にかかるメッセージ送信装置２１０の概略構成を示すブロック図である。本実施形態にかかるメッセージ送信装置２１０は、図２に示した第１実施形態にかかるメッセージ送信装置１１０と実質的に同一の内部構成を有するものであって、メッセージ生成部２１１、認証子生成鍵管理部２１２、メッセージ保持部２１３、送信予告情報生成部２１４、送信情報生成部２１５、受信証明検証部２１６、受信部２１７及び送信部２１８により構成される。以下では、本実施形態にかかるメッセージ送信装置２１０の構成要素について、第１実施形態にかかるメッセージ送信装置１１０の該当する構成要素と異なる点についてのみ説明する。

【０１０１】

（メッセージ生成部２１１）

メッセージ生成部２１１は、メッセージ送信装置（サーバ）２１０がメッセージ受信装置（ノード）２２０に対して送信するメッセージを生成するための機能部である。メッセージ生成部２１１は、生成したメッセージＭを送信予告情報生成部２１４に渡す点を除いて、上述した第１実施形態にかかるメッセージ生成部１１１と実質的に同一の機能を有する。

【０１０２】

（認証子生成鍵管理部２１２）

認証子生成鍵管理部２１２は、メッセージの認証子生成に用いられる認証子生成鍵鎖列K_i（$0 \leqq i \leqq m$，$m \geqq 1$）を管理するための機能部であって、上述した第１実施形態にかかる認証子生成鍵管理部１１２と実質的に同一の機能を有する。

【０１０３】

（メッセージ保持部２１３）

メッセージ保持部２１３は、メッセージ受信装置２２０に送信するメッセージＭを保持するための記憶部である。本実施形態のメッセージ保持部２１３は、送信予告情報生成部２１４から与えられる情報と、送信情報生成部２１５に与える情報とが、メッセージＭである点を除いて、上述した第１実施形態にかかるメッセージ保持部１１３と実質的に同一の機能を有する。

【０１０４】

（送信予告情報生成部２１４）

送信予告情報生成部２１４は、任意のデータに対する第１認証子と第２認証子とからなる送信予告情報を生成するための機能部であって、以下の点を除き、上述した第１実施形態にかかる送信予告情報生成部１１４と実質的に同一の機能を有する。本実施形態の送信予告情報生成部２１４は、メッセージ生成部２１１より与えられるメッセージＭに対する第１認証子及び第２認証子を生成し、送信情報生成部２１５に与える。また、メッセージＭをメッセージ保持部２１３へ与える。

【０１０５】

（送信情報生成部２１５）

送信情報生成部２１５は、各部からメッセージ受信装置２２０に対して送信するデータを収集し、収集したデータを送信するための送信情報を生成するための機能部である。送信情報生成部２１５は、メッセージＭに対する第１認証子及び第２認証子を送信予告情報生成部２１４から受け取り、受け取った第１認証子及び第２認証子からなる送信情報を生成し、生成した送信情報を受信証明検証部２１６と送信部２１８とに渡す。また、メッセージ保持部２１３からメッセージＭを受け取ると、メッセージＭを１以上のデータブロックM_j（$1 \leqq j \leqq n$，$n \geqq 1$）に分割し、各データブロックM_jを含む送信情報を生成し、生成した送信情報を順次、受信証明検証部２１６と送信部２１８とに渡す。各データブロックM_jを含む送信情報には、送信順を示すシーケンス番号ｊが付加されるようにしてもよい。また、認証子生成鍵管理部２１２より認証子生成鍵K_aを受け取ると、認証子生成鍵K_aを含む送信情報を生成し、生成した送信情報を受信証明検証部２１６と送信部２１８とに渡す。

【０１０６】

（受信証明検証部２１６）

受信証明検証部２１６は、メッセージ受信装置２２０から受信した受信証明情報を用いて、送信した送信情報が対象となるメッセージ受信装置２２０によって受信されたか否かを検証するための機能部である。本実施形態にかかる受信証明検証部２１６は、送信情報生成部２１５から受け取った送信予告情報（第１認証子及び第２認証子）を用いて、メッセージ受信装置２２０から受信部２１７を通して受信する受信証明情報を検証する。メッセージ受信装置２２０において送信予告情報が正しく受信されたことが確認された場合、受信証明検証終了メッセージを認証子生成鍵管理部２１２とメッセージ保持部２１３とに送信する。

【０１０７】

また、受信証明検証部２１６は、送信情報生成部２１５から認証子生成鍵K_aまたはデータブロックM_jを受け取って、それらの情報がメッセージ受信装置２２０において正しく受信されたか否かを検証する。具体的には、送信予告情報の場合と同様に、メッセージ受信装置２２０から受信証明情報を受信し、その受信証明情報を認証子生成鍵K_aまたはデータブロックM_jを用いて検証するようにしてもよいし、あるいは、メッセージ受信装置２２０からＡＣＫ／ＮＡＣＫを返信されることにより、送信情報がメッセージ受信装置２２０に到達したか否かを検知するようにしてもよい。また、送信情報が到達していない場合は、送信部２１８に認証子生成鍵K_aまたはデータブロックM_jを与え、再送信するようにしてもよい。また、ここでは、上述した送信予告情報の受信確認の場合と異なり、受信が確認された場合の受信証明検証終了メッセージの送信は行われない。

【０１０８】

（受信部２１７、送信部２１８）

受信部２１７及び送信部２１８は、それぞれ上述した第１実施形態にかかる受信部１１７及び１１８と実質的に同一の機能を有するものであるため、重複説明を省略する。

【０１０９】

以上、本実施形態にかかるメッセージ送信装置２１０の各部について、第１実施形態の該当する各部との相違点を中心に説明した。なお、メッセージ生成部２１１、認証子生成鍵管理部２１２、送信予告情報生成部２１４、送信情報生成部２１５、受信証明検証部２１６、受信部２１７及び送信部２１８は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、メッセージ保持部２１３は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。

【０１１０】

（メッセージ受信装置２２０）

次に、図１３を参照して、本実施形態にかかるメッセージ認証システムのメッセージ受信装置２２０について説明する。図１３は、本実施形態にかかるメッセージ受信装置２２０の概略構成を示すブロック図である。本実施形態にかかるメッセージ受信装置２２０は、図１３に示すように、受信部２２１、受信証明情報生成部２２２、認証子生成鍵検証部２２３、送信予告情報保持部２２４、第１認証子認証部２２５、メッセージ認証部２２６、送信部２２７及びメッセージ復元部２２８により構成される。

【０１１１】

本実施形態にかかるメッセージ受信装置２２０を構成する各部のうち、受信証明情報生成部２２２、メッセージ認証部２２６及びメッセージ復元部２２８を除いては、上述した第１の実施形態にかかるメッセージ受信装置１２０の各部に該当する構成要素と実質的に同一の構成を有するものであるため、詳細説明は省略する。以下、本実施形態にかかるメッセージ受信装置２２０の受信証明情報生成部２２２、メッセージ認証部２２６及びメッセージ復元部２２８について説明する。

【０１１２】

（受信証明情報生成部２２２）

受信証明情報生成部２２２は、受信部２２１より与えられた送信情報を確かに受信したことをメッセージ送信装置２１０に証明するための受信証明情報を生成するための機能部である。本実施形態にかかる受信証明情報生成部２２２は、以下の点を除き、上述した第１実施形態にかかる受信証明情報生成部１２２と実質的に同一の機能を有する。

【０１１３】

本実施形態にかかる受信証明情報生成部２２２は、受信部２２１から受け取った送信情報が、認証子生成鍵K_aまたはデータブロックM_jの場合、それらの情報を確かに受信したことをメッセージ送信装置２１０に証明するために、ＡＣＫメッセージやＮＡＣＫメッセージを生成し、送信部２２７を通して送信してもよい。

【０１１４】

また、受信証明情報生成部２２２は、受信部２２１より与えられたデータブロックM_jをメッセージ復元部２２８へ与える。

【０１１５】

（メッセージ認証部２２６）

メッセージ認証部２２６は、メッセージ送信装置２１０から受信したメッセージが正当なメッセージであるかを認証するための機能部である。本実施形態にかかるメッセージ認証部２２６は、以下の点を除き、上述した第１実施形態にかかるメッセージ認証部１２６と実質的に同一の機能を有する。本実施形態にかかるメッセージ認証部２２６は、メッセージ復元部２２８よりメッセージMを与えられ、第１認証子認証部１２５より与えられた認証子生成鍵K_aまたはK_a’と第１認証子とを用いて、メッセージMがメッセージ送信装置２１０から送信された正しいメッセージであることを認証する。

【０１１６】

（メッセージ復元部２２８）

メッセージ復元部２２８は、メッセージ送信装置２１０より分割して送信されたデータブロックM_jから、元のメッセージMを復元するための機能部である。メッセージ復元部２２８は、受信証明情報生成部２２２よりデータブロックM_jを受け取り、メッセージMを復元する。また、メッセージ復元部２２８は、復元されたメッセージMをメッセージ認証部２２６へ与える。

【０１１７】

以上、本実施形態にかかるメッセージ受信装置２２０の各部について説明した。なお、受信部２２１、受信証明情報生成部２２２、認証子生成鍵検証部２２３、第１認証子認証部２２５、メッセージ認証部２２６、送信部２２７及びメッセージ復元部２２８は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、送信予告情報保持部２２４は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。

【０１１８】

次に、図１４～図１９に基づいて、本実施形態にかかるメッセージ認証システムにより実行されるメッセージ認証処理の一例を説明する。ここで、図１４及び１５は、本実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。また、図１６は、同実施形態にかかるメッセージ認証処理のステップＳ２５４における状態を示した説明図である。同様に、図１７、１８及び１９は、それぞれステップＳ２５６、ステップＳ２６２及びステップＳ２７０における状態を示した説明図である。

【０１１９】

まず、ステップＳ２５０で、メッセージ送信装置２１０のメッセージ生成部２１１において、送信するメッセージMを生成する。生成されたメッセージMは、送信予告情報生成部２１４に渡される。

【０１２０】

次いで、ステップＳ２５１で、送信予告情報生成部２１４において、メッセージMに対する第１認証子を生成する。ここでは、ネットワークに未公開の現在のアクティブ鍵K_aに一方向性関数Gを適用して求められた値$K_a' = G(K_a)$を用いて第１認証子ＭＡＣ（K_a'，M）を生成するものとする。ここで、関数Gは、システムで公開された関数であるものとする。

【０１２１】

次いで、ステップＳ２５２で、第１認証子ＭＡＣ（K_a'，M）に対する第２認証子（第１認証子の正当性を証明するための情報）を生成する。ここでは、現在のアクティブ鍵K_aを用いて第２認証子ＭＡＣ（K_a，ＭＡＣ（K_a'，M））を生成するものとする。生成された第１認証子及び第２認証子は、送信情報生成部２１５に渡される。

【０１２２】

次いで、ステップＳ２５３で、送信情報生成部２１５において、第１認証子ＭＡＣ（K_a'，Ｍ）及び第２認証子ＭＡＣ（K_a，ＭＡＣ（K_a'，Ｍ））を含む送信情報を生成する。

【０１２３】

次いで、図１６に示すように、ステップＳ２５４で、生成した送信情報２３０を送信部２１８を通してメッセージ受信装置２２０に送信する。送信後、メッセージ送信装置２１０は、ステップＳ２５５で、送信した送信情報２３０を格納する。

【０１２４】

メッセージ受信装置２２０は、受信部２２１を通して受信した送信情報２３０を、受信証明情報生成部２２２に与える。受信証明情報生成部２２２は、ステップＳ２５６で、送信情報２３０に対する受信証明情報２３１を生成し、図１７に示すように、メッセージ送信装置２１０に送信する。次いで、ステップＳ２５７で、送信情報２３０に含まれる送信予告情報を送信予告情報保持部２２４に渡し、受信順に格納する。

【０１２５】

ステップＳ２５６でメッセージ受信装置２２０から受信証明情報２３１を受け取ったメッセージ送信装置２１０は、ステップＳ２５８で、受信証明検証部２１６において受信証明情報２３１の検証を行う。検証により、受信が確認された場合は、ステップＳ２５９に進み、メッセージＭを送信することが決定される。次いで、ステップＳ２６０で、送信予告情報の生成に用いられた認証子生成鍵K_aをネットワークに公開することが決定される。さらに、ステップＳ２６１で、アクティブ鍵K_aをK_{a+1}に更新する。

【０１２６】

ステップＳ２５８において受信証明情報２３１を検証した結果、受信が確認できなかった場合は、ステップＳ２５５に戻って、送信予告情報２３０をメッセージ受信装置２２０に対して再送信するようにしてもよい。

【０１２７】

次いで、ステップＳ２６２で、図１８に示すように、メッセージ送信装置２１０からメッセージ受信装置２２０に対して認証子生成鍵K_aを含む送信情報２３２を送信する。メッセージ受信装置２２０は、送信情報２３２の受信を確認し、図１８に示すように、ＡＣＫ／ＮＡＣＫメッセージ２３３をメッセージ送信装置２１０に返信するようにしてもよい。送信後、ステップＳ２６３で、メッセージ送信装置２１０は認証子生成鍵K_aを格納する。

【０１２８】

認証子生成鍵K_aを受信したメッセージ受信装置２２０は、ステップＳ２６４で、認証子生成鍵K_aを認証する。認証子生成鍵K_aが正常に認証されたら、ステップＳ２６５で、認証子生成鍵K_aを格納する。

【０１２９】

次いで、ステップＳ２６６で、送信予告情報保持部２２４に保持されている送信予告情報に含まれる第１認証子の認証を行う。送信予告情報保持部２２４は、保持している送信予告情報を受信した順に第１認証子認証部２２５に与え、第１認証子認証部２２５において認証が行われる。例えば、第１認証子認証部２２５は、認証子生成鍵K_aを用いて第１認証子に対する認証子を生成し、生成された認証子が第２認証子と一致するか否かを判定することにより、第１認証子を認証する。

【０１３０】

認証が正常に行われなかった場合は、ステップＳ２６７に進み、その送信予告情報を破棄する。認証が正常に行われた場合は、ステップＳ２６８に進み、認証された送信予告情報以外の送信予告情報を破棄する。

【０１３１】

一方、ステップＳ２６９で、メッセージ送信装置２１０は、メッセージＭからデータブロックM_jを生成する。次いで、図１９に示すように、ステップＳ２７０で、生成したデータブロックM_jを含む送信情報２３４を順次メッセージ受信装置２２０に対して送信す

る。メッセージ受信装置２２０は、送信情報２３４の受信を確認し、図１９に示すように、ＡＣＫ／ＮＡＣＫメッセージ２３５をメッセージ送信装置２１０に返信するようにしてもよい。送信後、ステップＳ２７１で、メッセージ送信装置２１０は認証子生成鍵K_aを格納する。

【０１３２】

メッセージ送信装置２１０からメッセージ受信装置２２０に全てのデータブロックM_jが送信された後、ステップＳ２７２で、メッセージ復元部２２８においてデータブロックM_jからメッセージＭを復元する。

【０１３３】

次いで、ステップＳ２７３で、メッセージ認証部２２６においてメッセージＭの認証を行う。メッセージ認証部２２６は、例えば、ステップＳ２６４で認証された認証子生成鍵K_aにシステムで規定された一方向性関数Ｇを適用して求めた値K_a'を用いて、メッセージＭに対する認証子を生成し、生成された値がステップＳ２６６で認証された第１認証子と一致するかを判定することにより、メッセージＭの認証を行う。

【０１３４】

以上、本実施形態にかかるメッセージ認証システムにより実行されるメッセージ認証処理の一例を説明した。

【０１３５】

本実施形態の構成によれば、メッセージ送信装置は、複数のデータブロックM_j（$1 \leqq j \leqq n$，$n \geqq 1$）に分割する前のメッセージＭ全体に対して生成した第１認証子と、第１認証子の正当性を証明するための第２認証子をメッセージ受信装置に送り、上記２つの認証子がメッセージ受信装置に到達したことを確認した後で、認証子生成鍵を公開し、その後、データブロックM_1、M_2、…、M_nを順次送信する。

【０１３６】

このように、１つのメッセージに対して１つの認証子を送信するようにしたことで、各パケットに第１認証子及び第２認証子と認証子生成鍵を含めて送信する第１実施形態と比較すると、１つのパケットに含めることができるメッセージのデータブロックのサイズを大きくすることができる。

【０１３７】

（第３の実施形態）

次に、図２０及び２１を参照して、本発明の第３の実施形態にかかるメッセージ認証システムについて説明する。本実施形態にかかるメッセージ認証システムでは、メッセージ送信装置は、最初のパケットに対して送信予告情報を生成し、メッセージ受信装置は、最初のパケットを認証したことをコミットメントとすることによって、その後に受信するパケットを認証するようにしたことを特徴とするものである。

【０１３８】

（メッセージ送信装置３１０）

まず、図２０を参照して、本実施形態にかかるメッセージ認証システムのメッセージ送信装置３１０について説明する。図２０は、本実施形態にかかるメッセージ送信装置３１０の概略構成を示すブロック図である。本実施形態にかかるメッセージ送信装置３１０は、図２０に示すように、メッセージ生成部３１１、認証子生成鍵管理部３１２、メッセージ保持部３１３、送信予告情報生成部３１４、送信情報生成部３１５、受信証明検証部３１６、受信部３１７、送信部３１８及び認証情報付加部３１９により構成される。

【０１３９】

本実施形態にかかるメッセージ送信装置３１０を構成する各部は、上述した第１実施形態にかかるメッセージ送信装置の各部に該当する構成要素と実質的に同一の構成を有する。以下では、本実施形態にかかるメッセージ送信装置３１０の構成要素のうち、第１実施形態にかかるメッセージ送信装置１１０の該当する構成要素と機能が異なるメッセージ生成部３１１、メッセージ保持部３１３、送信予告情報生成部３１４、送信情報生成部３１５、受信証明検証部３１６、認証情報付加部３１９についてのみ説明する。

【０１４０】
（メッセージ生成部３１１）
メッセージ生成部３１１は、メッセージ送信装置（サーバ）３１０がメッセージ受信装置（ノード）３２０に対して送信するメッセージを生成するための機能部である。メッセージ生成部３１１は、生成したメッセージＭを１以上のデータブロックM_j（$1 \leqq j \leqq n$，$n \geqq 1$）に分割し、分割された各データブロックM_jを認証情報付加部３１９に渡す点を除いて、上述した第１実施形態にかかるメッセージ生成部１１１と実質的に同一の機能を有する。
【０１４１】
（メッセージ保持部３１３）
メッセージ保持部３１３は、メッセージ受信装置３２０に送信するメッセージのデータブロックを保持するための記憶部であって、本実施形態のメッセージ保持部３１３は、以下の点を除いて、上述した第１実施形態にかかるメッセージ保持部１１３と実質的に同一の機能を有する。本実施形態にかかるメッセージ保持部３１３は、認証情報付加部３１９より与えられた情報（第１認証情報A_0、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）、及びM_n）を保持する。メッセージ保持部３１３は、受信証明検証部３１６より受信証明検証終了メッセージを受信すると、保持している第１認証情報A_0、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）、及びM_nを順次送信情報生成部３１５へ与える。
【０１４２】
（送信予告情報生成部３１４）
送信予告情報生成部３１４は、任意のデータに対する第１認証子と第２認証子とからなる送信予告情報を生成するための機能部であって、以下の点を除き、上述した第１実施形態にかかる送信予告情報生成部１１４と実質的に同一の機能を有する。本実施形態にかかる送信予告情報生成部３１４は、認証情報付加部３１９より与えられた第１認証情報A_0に対して、第１認証子及び第２認証子を生成し、送信情報生成部３１５に与える。また、メッセージ生成部３１１より与えられた情報（第１認証情報A_0、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）、及びM_n）をメッセージ保持部３１３に与える。
【０１４３】
（送信情報生成部３１５）
送信情報生成部３１５は、メッセージ受信装置２２０に対する送信情報を生成するための機能部であって、以下の点を除き、上述した第１実施形態にかかる送信情報生成部１１５と実質的に同一の機能を有する。本実施形態にかかる送信情報生成部３１５は、メッセージ保持部３１３から第１認証情報A_0、データブロック（M_j，A_j）、またはM_nのいずれかを与えられ、これらの情報をそれぞれ含む送信情報を生成する。
【０１４４】
（受信証明検証部３１６）
受信証明検証部３１６は、送信した送信情報が対象となるメッセージ受信装置２２０によって受信されたか否かを検証するための機能部であって、以下の点を除き、上述した第１実施形態にかかる受信証明検証部１１６と実質的に同一の機能を有する。本実施形態にかかる受信証明検証部３１６は、送信情報生成部３１５から送信予告情報（第１認証子及び第２認証子）を受け取る場合、第１実施形態にかかる受信証明検証部１１６と実質的に同一の動作を行う。
【０１４５】
また、送信情報生成部３１５から認証子生成鍵K_a、第１認証情報A_0、データブロック（M_j，A_j）、またはM_nのいずれかを与えられる場合、受信証明検証部３１６は、それらの情報がメッセージ受信装置３２０において正しく受信されたか否かを検証する。具体的には、送信予告情報の場合と同様に、メッセージ受信装置３２０から受信証明情報を受信し、その受信証明情報を認証子生成鍵K_a、第１認証情報A_0、データブロック（M_j，A_j）、またはM_nを用いて検証するようにしてもよい。あるいは、メッセージ受信装置３２０からＡＣＫ／ＮＡＣＫを返信されることにより、送信情報がメッセージ受信

装置３２０に到達したか否かを検知するようにしてもよい。また、送信情報が到達していない場合は、送信部３１８に認証子生成鍵K_a、第１認証情報A_0、データブロック（M_j，A_j）、またはM_nを与え、再送信するようにしてもよい。また、ここでは、上述した送信予告情報の受信確認の場合と異なり、受信が確認された場合の受信証明検証終了メッセージの送信は行われない。

【０１４６】

（認証情報付加部３１９）

認証情報付加部３１９は、メッセージＭの各データブロックM_jに認証情報を付加するための機能部である。認証情報付加部３１９は、メッセージ生成部３１１からデータブロックM_j（$1 \leqq j \leqq n$）を与えられ、データブロックM_jに対する認証情報を生成する。認証情報は、例えば、各データブロックから生成されたハッシュ値であってもよい。図２２は、認証情報付加部３１９によりデータブロックに付加される認証情報を説明するための説明図である。例えば、図２２に示すように、認証情報付加部３１９は、生成した全ての情報（第１認証情報A_0、データブロック（M_j，A_j）及びM_n）をメッセージ保持部３１３へ与え、第１認証情報A_0を、送信予告情報生成部３１４へ与える。

【０１４７】

以上、本実施形態にかかるメッセージ送信装置３１０の各部について、第１実施形態の該当する各部との相違点を中心に説明した。なお、メッセージ生成部３１１、認証子生成鍵管理部３１２、送信予告情報生成部３１４、送信情報生成部３１５、受信証明検証部３１６、受信部３１７、送信部３１８及び認証情報付加部３１９は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、メッセージ保持部３１３は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。

【０１４８】

（メッセージ受信装置３２０）

次に、図２１を参照して、本実施形態にかかるメッセージ認証システムのメッセージ受信装置３２０について説明する。図２１は、本実施形態にかかるメッセージ受信装置３２０の概略構成を示すブロック図である。本実施形態にかかるメッセージ受信装置３２０は、図２１に示すように、受信部３２１、受信証明情報生成部３２２、認証子生成鍵検証部３２３、送信予告情報保持部３２４、第１認証子認証部３２５、メッセージ認証部３２６、送信部３２７及び認証情報認証部３２９により構成される。

【０１４９】

本実施形態にかかるメッセージ受信装置３２０を構成する各部は、上述した第１の実施形態にかかるメッセージ受信装置１２０の各部に該当する構成要素と実質的に同一の構成を有する。以下では、本実施形態にかかるメッセージ受信装置３２０の受信部３２１、認証子生成鍵検証部３２３及び送信部３２７を除く構成要素について、第１実施形態にかかるメッセージ受信装置１２０の各部に該当する構成要素と異なる点についてのみ説明する。

【０１５０】

（受信証明情報生成部３２２）

受信証明情報生成部３２２は、送信情報を確かに受信したことをメッセージ送信装置３１０に証明するための受信証明情報を生成するための機能部であって、以下の点を除き、上述した第１実施形態にかかる受信証明情報生成部１２２と実質的に同一の機能を有する。本実施形態にかかる受信証明情報生成部３２２は、第１認証情報A_0を認証情報認証部３２９へ、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）及びM_nをメッセージ認証部３２６へ与える。受信部３２１から受け取った送信情報が、第１認証情報A_0を含まない情報である場合、受信証明情報生成部３２２は、それらの情報を確かに受信したことをメッセージ送信装置３１０に証明するために、ＡＣＫメッセージやＮＡＣＫメッセージを生成し、送信部３２７を通して送信してもよい。

【０１５１】
（送信予告情報保持部３２４）
送信予告情報保持部３２４は、メッセージ送信装置３１０から受信した送信予告情報（第１認証子及び第２認証子）を保持するための記憶部であって、以下の点を除き、上述した第１実施形態にかかる送信予告情報保持部１２４と実質的に同一の機能を有する。本実施形態にかかる送信予告情報保持部３２４は、保持している送信予告情報（第１認証子及び第２認証子）を、第１認証情報A_0に対する送信予告情報として、受信した順番に第１認証子認証部３２５に与える。
【０１５２】
（第１認証子認証部３２５）
第１認証子認証部３２５は、メッセージ送信装置３１０より与えられた送信予告情報に含まれる第１認証子が正当なものであるか否かを検証するための機能部であって、以下の点を除き、上述した第１実施形態にかかる第１認証子認証部１２５と実質的に同一の機能を有する。本実施形態にかかる第１認証子認証部３２５は、送信予告情報保持部３２４より第１認証情報A_0に対する第１認証子及び第２認証子を受信した順番に与えられる。
【０１５３】
（メッセージ認証部３２６）
メッセージ認証部３２６は、受信証明情報生成部３２２より与えられたデータブロックM_jが（$1 \leqq j \leqq n$）が、メッセージ送信装置が生成した正しいデータブロックM_jであることを認証するための機能部である。メッセージ認証部３２６は、例えば、受信証明情報生成部３２２より与えられたデータブロック（M_1，A_1）に対するハッシュ値を生成し、生成されたハッシュ値と、認証情報認証部３２９より与えられた認証情報A_0が一致するか否かを判定することで、データブロック（M_1，A_1）を認証する。同様に、例えば、受信証明情報生成部３２２より与えられたデータブロック（M_j，A_j）（$2 \leqq j \leqq n-1$）に対するハッシュ値を生成し、生成されたハッシュ値が、既に認証済みの認証情報A_{j-1}と一致するか否かを判定することで、データブロック（M_j，A_j）を認証する。最後に、例えば、受信証明情報生成部３２２より与えられたデータブロックM_nに対するハッシュ値を生成し、生成されたハッシュ値が、既に認証済みの認証情報A_{n-1}と一致するか否かを判定することで、データブロックM_nを認証する。
【０１５４】
（認証情報認証部３２９）
認証情報認証部３２９は、受信証明情報生成部３２２より与えられた第１認証情報A_0が、メッセージ送信装置３１０が送信した正当な認証情報であることを認証するための機能部である。認証情報認証部３２９は、例えば、第１認証子認証部３２５より与えられた認証子生成鍵K_a'またはK_aを用いて、受信証明情報生成部３２２より与えられた第１認証情報A_0に対する認証子を生成し、生成した認証子と第１認証子認証部３２５より与えられた第１認証子とが一致するか否かを判定することにより第１認証情報A_0を認証する。第１認証情報A_0が正常に認証されたら、第１認証情報A_0をメッセージ認証部３２６へ与える。
【０１５５】
以上、本実施形態にかかるメッセージ受信装置３２０の各部について説明した。なお、受信部３２１、受信証明情報生成部３２２、認証子生成鍵検証部３２３、第１認証子認証部３２５、メッセージ認証部３２６、送信部３２７及び認証情報認証部３２９は、上述した各機能を実行可能なプログラムモジュールをコンピュータ等の情報処理装置にインストールしたソフトウェアで構成されてもよいし、あるいは、上述した各機能を実行可能なプロセッサ等のハードウエアで構成されてもよい。また、送信予告情報保持部３２４は、例えば、半導体メモリ、光ディスク、磁気ディスク等の各種の記憶媒体等により構成されてもよい。
【０１５６】
次に、図２３～図２８に基づいて、本実施形態にかかるメッセージ認証システムにより

実行されるメッセージ認証処理の一例を説明する。ここで、図２３及び２４は、本実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。また、図２５は、同実施形態にかかるメッセージ認証処理のステップＳ３５６における状態を示した説明図である。同様に、図２６、２７及び２８は、それぞれステップＳ３５８、ステップＳ３６４及びステップＳ３７２における状態を示した説明図である。

【０１５７】

まず、ステップＳ３５０で、メッセージ送信装置３１０のメッセージ生成部３１１において、送信するメッセージＭを生成する。次に、ステップＳ３５１で、メッセージＭを分割したデータブロックM_j（$1 \leqq j \leqq n$）を生成する。生成されたデータブロックM_jは、認証情報付加部３１９に与えられる。

【０１５８】

次いで、ステップＳ３５２で、認証情報付加部３１９において、認証情報A_j（$0 \leqq j \leqq n-1$）を生成する。認証情報A_jは、例えば、図２２に示すような手順によって生成される。まず、最後のデータブロックM_nのハッシュ値である認証情報A_{n-1}を生成し、データブロックM_{n-1}に付加する。さらに、認証情報A_{n-1}が付加されたデータブロック（M_{n-1}，A_{n-1}）のハッシュ値である認証情報A_{n-2}を生成し、データブロックM_{n-2}に付加する。これを繰り返すことにより、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）と認証情報A_0が生成される。ここで、最後に生成された認証情報A_0を第１認証情報と呼ぶ。生成された第１認証情報A_0は、送信予告情報生成部３１４に与えられる。また、生成された全ての情報（第１認証情報A_0、データブロック（M_j，A_j）及びM_n）がメッセージ保持部３１３へ与えられる。

【０１５９】

次いで、ステップＳ３５３において、送信予告情報生成部３１４において、第１認証情報A_0に対する第１認証子を生成する。ここでは、ネットワークに未公開の現在のアクティブ鍵K_aに一方向性関数Ｇを適用して求められた値$K_a' = G(K_a)$を用いて第１認証子ＭＡＣ（K_a'，A_0）を生成するとする。ここで、関数Ｇは、システムで公開された関数であるものとする。

【０１６０】

次いで、ステップＳ３５４で、第１認証子ＭＡＣ（K_a'，A_0）に対する第２認証子（第１認証子の正当性を証明するための情報）を生成する。ここでは、現在のアクティブ鍵K_aを用いて第２認証子ＭＡＣ（K_a，ＭＡＣ（K_a'，A_0））を生成するものとする。生成された第１認証子及び第２認証子は、送信情報生成部３１５に渡される。

【０１６１】

次いで、ステップＳ３５５で、送信情報生成部３１５において、第１認証子ＭＡＣ（K_a'，A_0）及び第２認証子ＭＡＣ（K_a，ＭＡＣ（K_a'，A_0））を含む送信情報を生成する。

【０１６２】

次いで、図２５に示すように、ステップＳ３５６で、生成した送信情報３３０を送信部３１８を通してメッセージ受信装置３２０に送信する。送信後、メッセージ送信装置３１０は、ステップＳ３５７で、送信した送信情報３３０を格納する。

【０１６３】

メッセージ受信装置３２０は、受信部３２１を通して受信した送信情報３３０を、受信証明情報生成部３２２に与える。受信証明情報生成部３２２は、ステップＳ３５８で、送信情報３３０に対する受信証明情報３３１を生成し、図２６に示すように、メッセージ送信装置３１０に送信する。次いで、ステップＳ３５９で、送信情報３３０に含まれる送信予告情報を送信予告情報保持部３２４に渡し、受信順に格納する。

【０１６４】

ステップＳ３５８でメッセージ受信装置３２０から受信証明情報３３１を受け取ったメッセージ送信装置３１０は、ステップＳ３６０で、受信証明検証部３１６において受信証明情報３３１の検証を行う。検証により、受信が確認された場合は、ステップＳ３６１に

進み、第１認証情報A_0、データブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）及びM_nを送信することが決定される。次いで、ステップＳ３６２で、送信予告情報の生成に用いられた認証子生成鍵K_aをネットワークに公開することが決定される。さらに、ステップＳ３６３で、アクティブ鍵K_aをK_{a+1}に更新する。

【０１６５】

次いで、ステップＳ３６４で、図２７に示すように、メッセージ送信装置３１０からメッセージ受信装置３２０に対して第１認証情報A_0と認証子生成鍵K_aとを含む送信情報３３２を送信する。メッセージ受信装置３２０は、送信情報３３２の受信を確認し、図２７に示すように、ＡＣＫ／ＮＡＣＫメッセージ３３３をメッセージ送信装置３１０に返信するようにしてもよい。送信後、ステップＳ３６５で、メッセージ送信装置３１０は第１認証情報A_0と認証子生成鍵K_aとを格納する。

【０１６６】

第１認証情報A_0及び認証子生成鍵K_aを受信したメッセージ受信装置３２０は、ステップＳ３６６で、認証子生成鍵K_aを認証する。認証子生成鍵K_aが正常に認証されたら、ステップＳ３６７で、認証子生成鍵K_aを格納する。

【０１６７】

次いで、ステップＳ３６８で、送信予告情報保持部３２４に保持されている送信予告情報に含まれる第１認証子の認証を行う。送信予告情報保持部３２４は、保持している送信予告情報を受信した順に第１認証子認証部３２５に与え、第１認証子認証部３２５において認証が行われる。例えば、第１認証子認証部３２５は、認証子生成鍵K_aを用いて第１認証子に対する認証子を生成し、生成された認証子が第２認証子と一致するか否かを判定することにより、第１認証子を認証する。

【０１６８】

認証が正常に行われなかった場合は、ステップＳ３６９に進み、その送信予告情報を破棄する。認証が正常に行われた場合は、ステップＳ３７０に進み、認証された送信予告情報以外の送信予告情報を破棄する。

【０１６９】

次いで、ステップＳ３７１で、認証情報認証部３２９において、第１認証情報A_0の認証を行う。例えば、認証情報認証部３２９は、第１認証子認証部３２５より与えられた認証子生成鍵K_a’またはK_aを用いて、受信証明情報生成部３２２より与えられた第１認証情報A_0に対する認証子を生成し、生成した認証子と第１認証子認証部３２５より与えられた第１認証子とが一致するか否かを判定することにより第１認証情報A_0を認証する。

認証された第１認証情報A_0は、メッセージ認証部３２６に渡される。

【０１７０】

一方、図２８に示すように、ステップＳ３７２で、メッセージ送信装置３１０からメッセージ受信装置３２０に対してデータブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）を含む送信情報３３４が送信される。データブロック（M_j，A_j）を受信したメッセージ受信装置３２０は、ステップＳ３７３で、メッセージ認証部においてデータブロック（M_j，A_j）の認証を行う。以下、メッセージ送信装置３１０が全てのデータブロック（M_j，A_j）（$1 \leqq j \leqq n-1$）を送信するまで、ステップＳ３７２及びステップＳ３７３の処理を繰り返す。

【０１７１】

データブロック（M_j，A_j）の認証は、例えば、メッセージ認証部３２６は、受信証明情報生成部３２２より与えられたデータブロック（M_1，A_1）に対するハッシュ値を生成し、生成されたハッシュ値と、認証情報認証部３２９より与えられた認証情報A_0が一致するか否かを判定することにより行われる。同様に、例えば、受信証明情報生成部３２２より与えられたデータブロック（M_j，A_j）（$2 \leqq j \leqq n-1$）に対するハッシュ値を生成し、生成されたハッシュ値が、既に認証済みの認証情報A_{j-1}と一致するか否かを判定することで、データブロック（M_j，A_j）を認証する。

【０１７２】
次いで、ステップＳ３７４において、メッセージ送信装置３１０において全てのデータブロック（M_j，A_j）（１≦ｊ≦ｎ－１）が送信されたと判断したら、ステップＳ３７５に進み、最後のデータブロックM_nをメッセージ受信装置３２０に対して送信する。
【０１７３】
メッセージ受信装置３２０においてデータブロックM_nが受信されると、メッセージ認証部３２６がデータブロックM_nを認証する。例えば、メッセージ認証部３２６は、受信証明情報生成部３２２より与えられたデータブロックM_nに対するハッシュ値を生成し、生成されたハッシュ値が、既に認証済みの認証情報A_{n-1}と一致するか否かを判定することにより、データブロックM_nを認証する。
【０１７４】
以上、本実施形態にかかるメッセージ認証システムにより実行されるメッセージ認証処理の一例を説明した。
【０１７５】
本実施形態の構成によれば、メッセージ送信装置は、最初のパケットに対して送信予告情報を生成し、メッセージ受信装置は、最初のパケットを認証できたことをコミットメントとすることによって、その後に受信するパケットを認証する。かかる構成により、各パケットに送信予告情報を含めて送信する第１実施形態の場合と比較すると、１つのパケットに含めることができるデータブロックのサイズを大きくすることができる。また、全データブロックから復元したメッセージに対して認証を行う第２実施形態と比較すると、全てのデータブロックが受信されていなくても、１つ前のデータブロックが認証されていることをコミットメントとして、各データブロック毎に認証を行うことができる。
【０１７６】
以上、添付図面を参照しながら本発明の好適な実施形態について説明したが、本発明は係る例に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。
【０１７７】
例えば、上述の第２、第３実施形態で、メッセージ受信装置では、認証できなかった場合に、送信部を通してエラーメッセージをメッセージ送信装置へ返信するようにしてもよい。
【０１７８】
また、上述の第３実施形態で、認証情報付加部は、データブロックM_j（１≦ｊ≦ｎ）のハッシュ値を葉としたＭｅｒｋｌｅ認証木を構築し、データブロックM_jに該当する葉の位置から根までに存在する全ての節の子の中で、上記葉から根に向かうルート以外に存在する子の情報を認証情報A_jとするようにしてもよい。また、ここで、第１認証情報A_0を、上記Ｍｅｒｋｌｅ認証木の根の値とするようにしてもよい。
【０１７９】
上記各実施形態においては、説明の簡単化のため、１つの認証子生成鍵で１つのメッセージを認証する場合について説明したが、本発明はかかる例に限定されない。例えば、１つの認証子生成鍵で複数のメッセージを認証するようにしてもよい。
【０１８０】
また、上記各実施形態においては、認証子生成鍵は、認証子生成鍵鎖列の鍵を用いて生成すると説明したが、本発明はかかる例に限定されない。例えば、認証子生成鍵には、認証子生成鍵鎖列の各鍵から派生した情報を用いるとし、メッセージ送信装置とメッセージ受信装置とが共にその情報を派生させるための方法を把握するようにしてもよい。
【０１８１】
また、上記各実施形態においては、メッセージ受信装置の説明の中で、マルチホップ通信において情報の中継を行う情報中継部について明記していないが、メッセージ受信装置がマルチホップ通信環境における中継装置である場合には、メッセージ受信装置は、受信

部から与えられた情報を送信部へ与えて中継先の装置へ転送する情報中継部を暗黙のうちに備えるものであることとする。

【図面の簡単な説明】

【０１８２】

【図１】本発明の第１実施形態にかかるメッセージ認証システムの概略構成を示すブロック図である

【図２】同実施形態にかかるメッセージ送信装置（サーバ）の概略構成を示すブロック図である。

【図３】同実施形態にかかるメッセージ受信装置（ノード）の概略構成を示すブロック図である。

【図４】認証子生成鍵管理部によって管理される認証子生成鍵鎖列を説明するための説明図である。

【図５】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

【図６】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

【図７】同実施形態にかかるメッセージ認証処理のステップＳ１５５における状態を示した説明図である。

【図８】同実施形態にかかるメッセージ認証処理のステップＳ１５５における状態を示した説明図である。

【図９】同実施形態にかかるメッセージ認証処理のステップＳ１６３における状態を示した説明図である。

【図１０】同実施形態にかかるメッセージ認証処理の送信情報再送時における状態を示した説明図である。

【図１１】同実施形態にかかるメッセージ認証処理システムの効果を説明するためのシーケンス図である。

【図１２】本発明の第２実施形態にかかるメッセージ送信装置の概略構成を示すブロック図である。

【図１３】同実施形態にかかるメッセージ受信装置の概略構成を示すブロック図である。

【図１４】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

【図１５】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

【図１６】同実施形態にかかるメッセージ認証処理のステップＳ２５４における状態を示した説明図である。

【図１７】同実施形態にかかるメッセージ認証処理のステップＳ２５６における状態を示した説明図である。

【図１８】同実施形態にかかるメッセージ認証処理のステップＳ２６２における状態を示した説明図である。

【図１９】同実施形態にかかるメッセージ認証処理のステップＳ２７０における状態を示した説明図である。

【図２０】本発明の第３実施形態にかかるメッセージ送信装置の概略構成を示すブロック図である。

【図２１】同実施形態にかかるメッセージ受信装置の概略構成を示すブロック図である。

【図２２】同実施形態にかかる認証情報付加部によりデータブロックに付加される認証情報を説明するための説明図である。

【図２３】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

【図２４】同実施形態にかかるメッセージ認証処理の流れを示すフローチャートである。

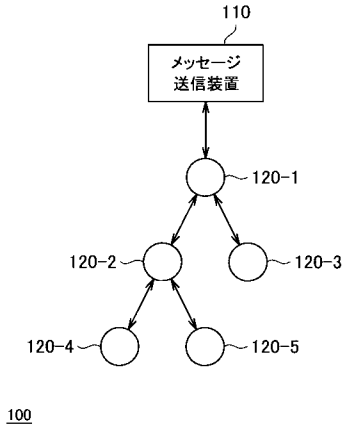
【図２５】同実施形態にかかるメッセージ認証処理のステップＳ３５６における状態を示した説明図である。

【図２６】同実施形態にかかるメッセージ認証処理のステップＳ３５８における状態を示した説明図である。

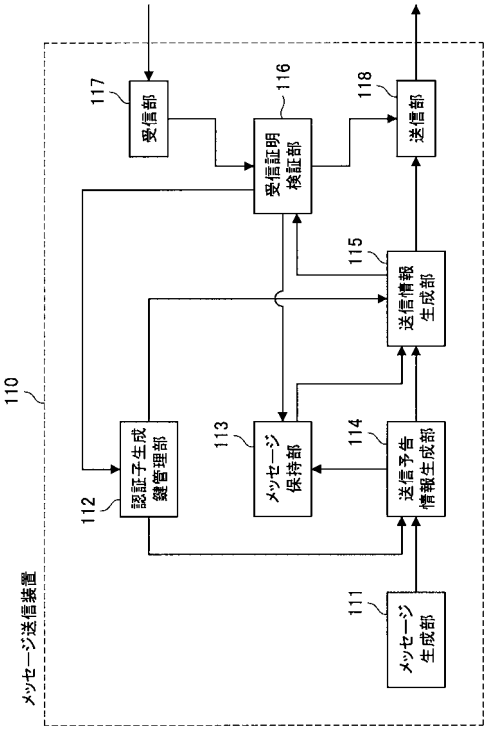
【図２７】同実施形態にかかるメッセージ認証処理のステップＳ３６４における状態を示した説明図である。

【図２８】同実施形態にかかるメッセージ認証処理のステップＳ３７２における状態を示した説明図である。
【図２９】従来のメッセージ認証方式の処理の流れを示すシーケンス図である。
【図３０】従来のメッセージ認証方式の処理における攻撃例を示すシーケンス図である。
【符号の説明】
【０１８３】
１００　メッセージ認証システム
１１０、２１０、３１０　メッセージ送信装置
１１１、２１１、３１１　メッセージ生成部
１１２、２１２、３１２　認証子生成鍵管理部
１１３、２１３、３１３　メッセージ保持部
１１４、２１４、３１４　送信予告情報生成部
１１５、２１５、３１５　送信情報生成部
１１６、２１６、３１６　受信証明検証部、
１１７、２１７、３１７、１２１、２２１、３２１　受信部
１１８、２１８、３１８、１２７、２２７、３２７　送信部
１２０、２２０、３２０　メッセージ受信装置
１２２、２２２、３２２　受信証明情報生成部
１２３、２２３、３２３　認証子生成鍵検証部
１２４、２２４、３２４　送信予告情報保持部
１２５、２２５、３２５　第１認証子認証部
１２６、２２６、３２６　メッセージ認証部
２２８　メッセージ復元部
３１９　認証情報付加部
３２９　認証情報認証部

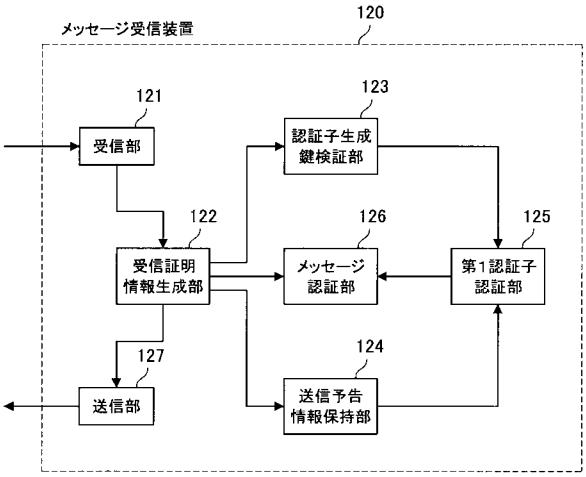
【図１】



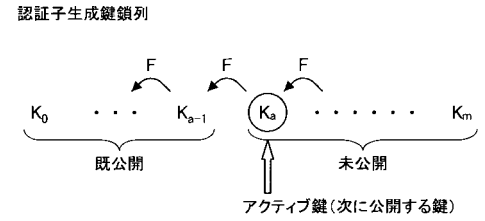
【図２】



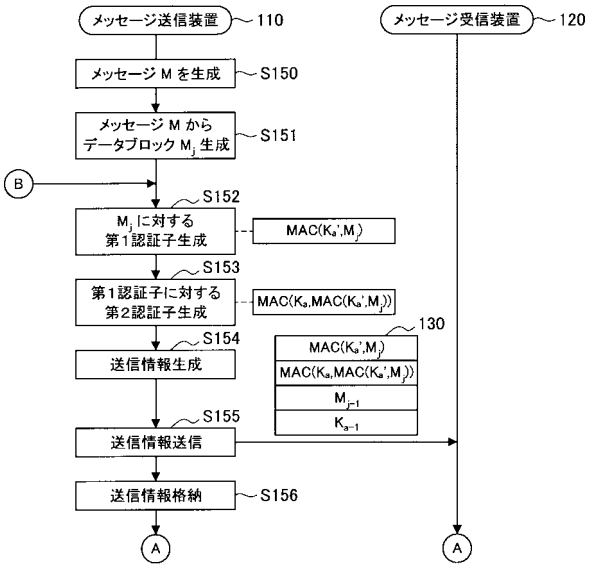
【図３】



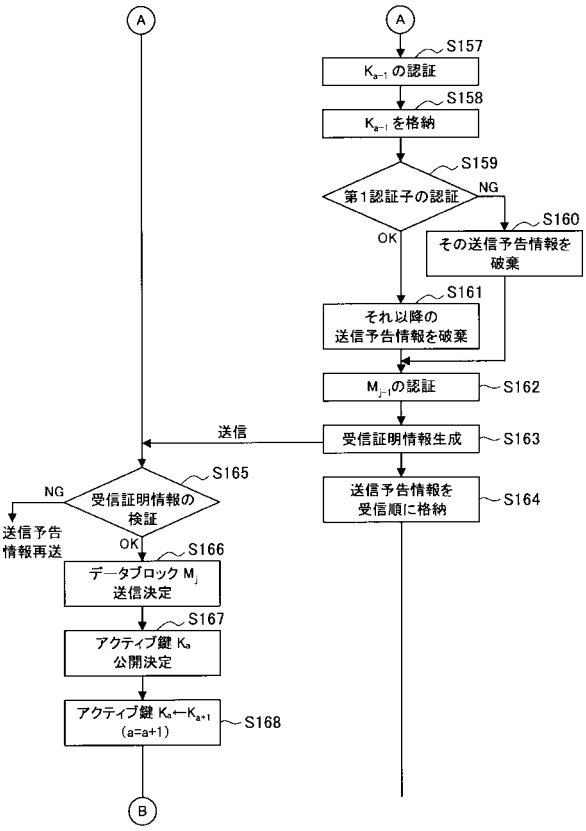
【図４】



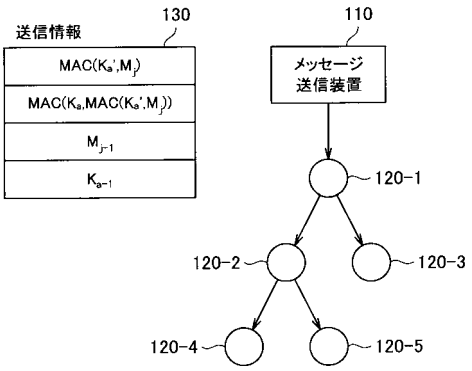
【図５】



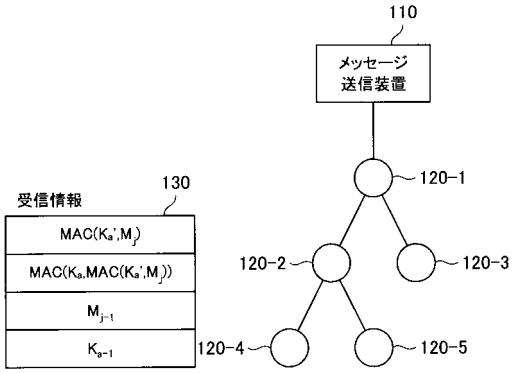
【図６】



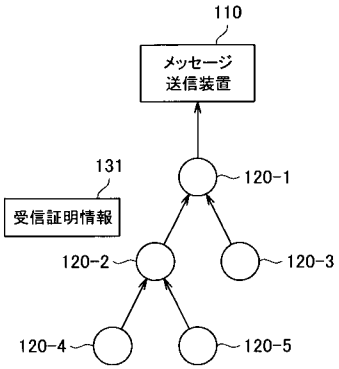
【図７】



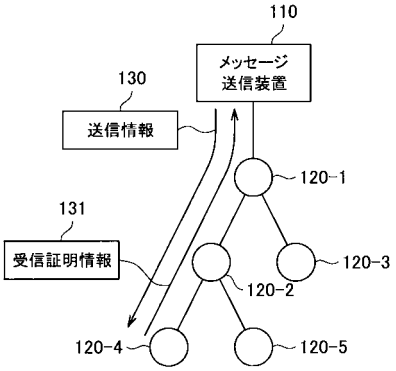
【図８】



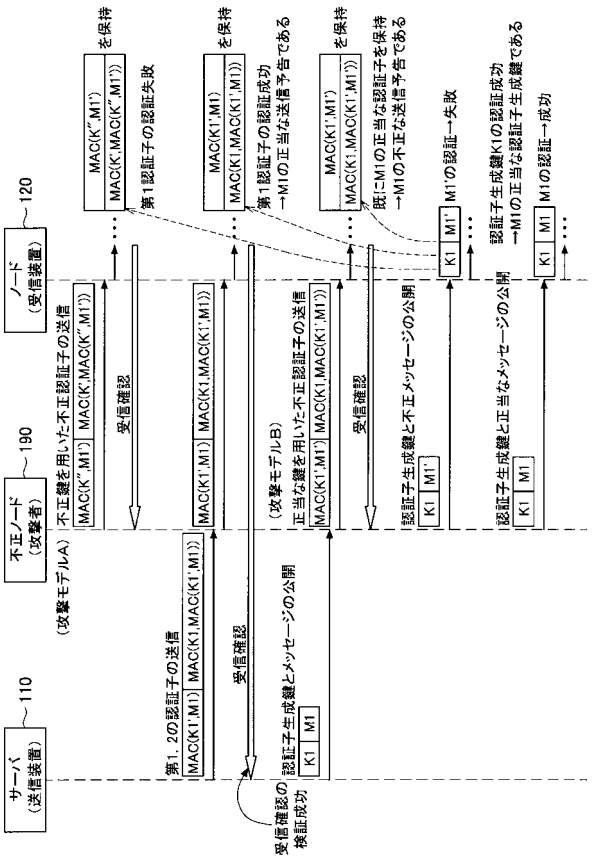
【図９】



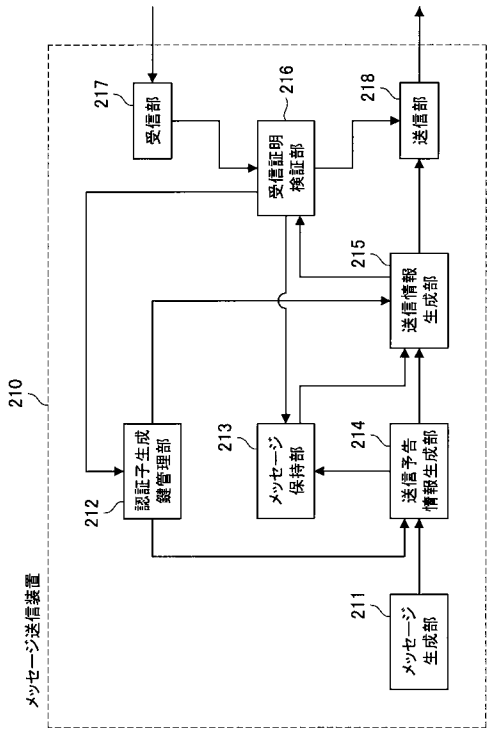
【図１０】



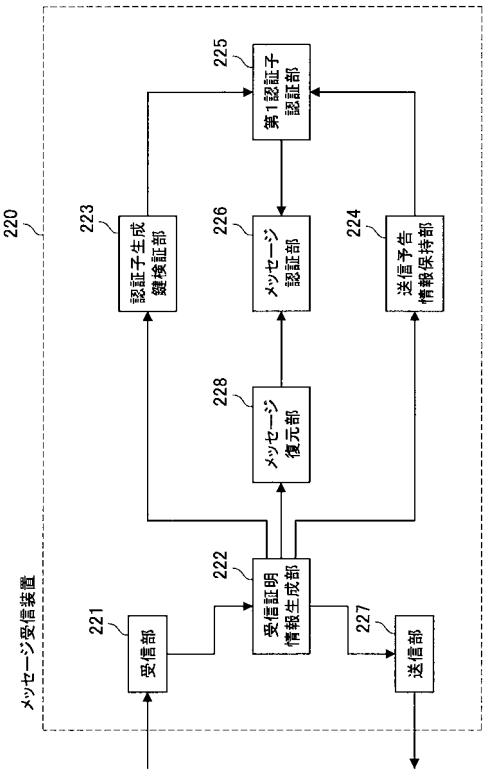
【図１１】



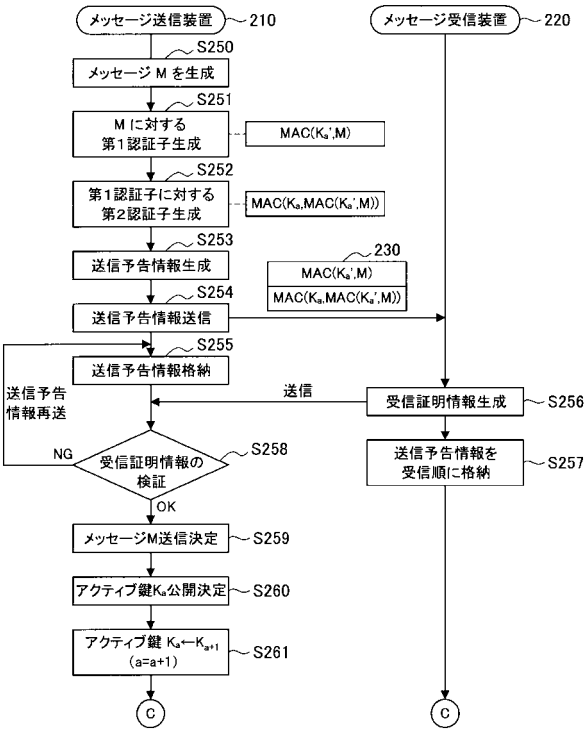
【図１２】



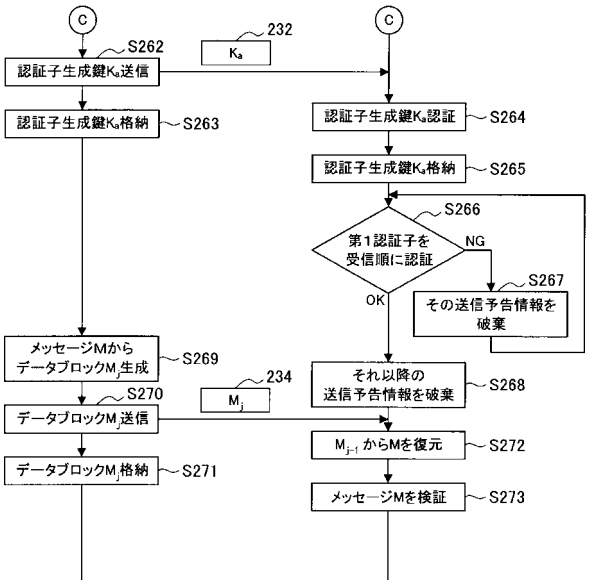
【図１３】



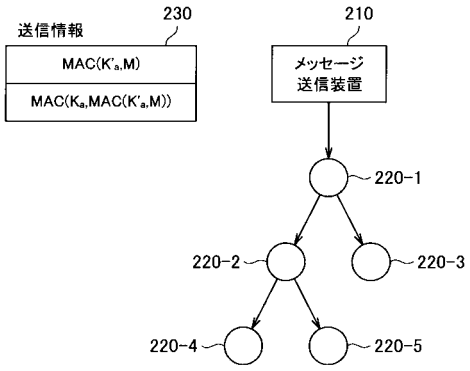
【図１４】



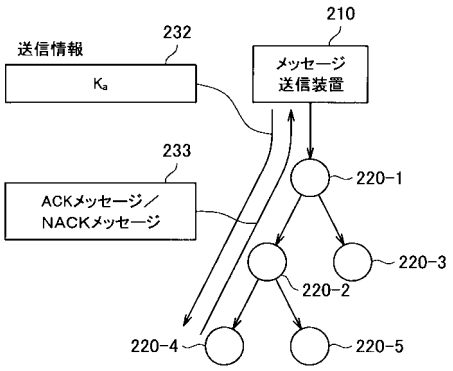
【図１５】



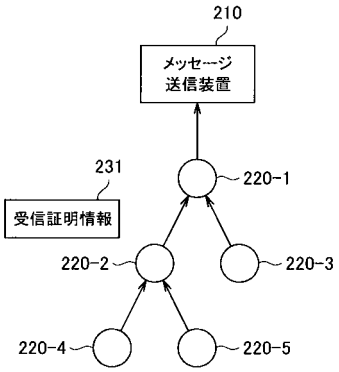
【図１６】



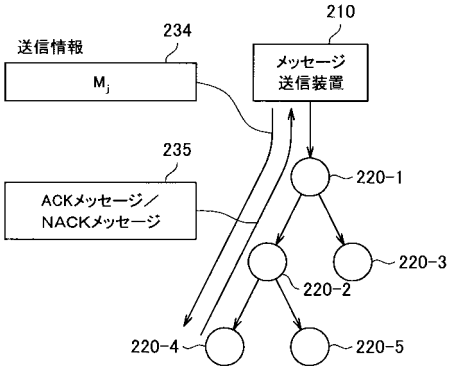
【図１８】



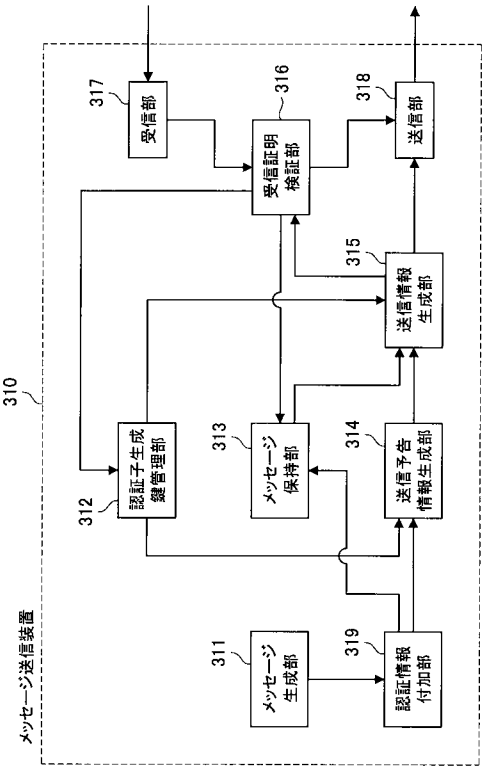
【図１７】



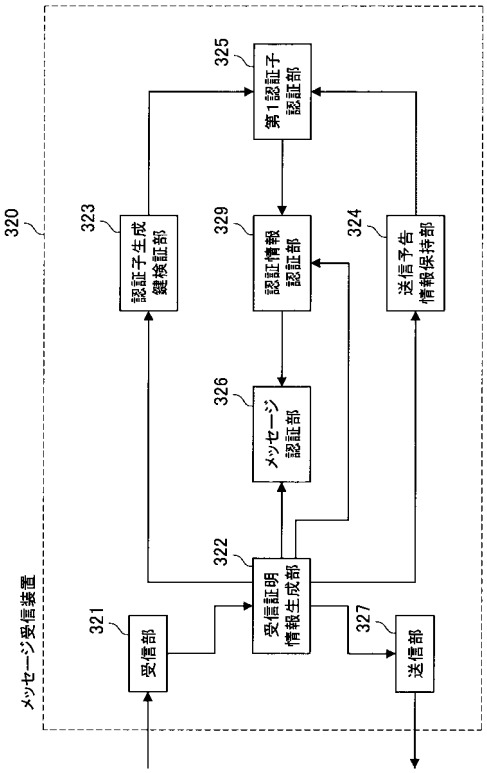
【図１９】



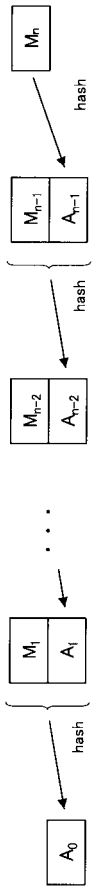
【図２０】



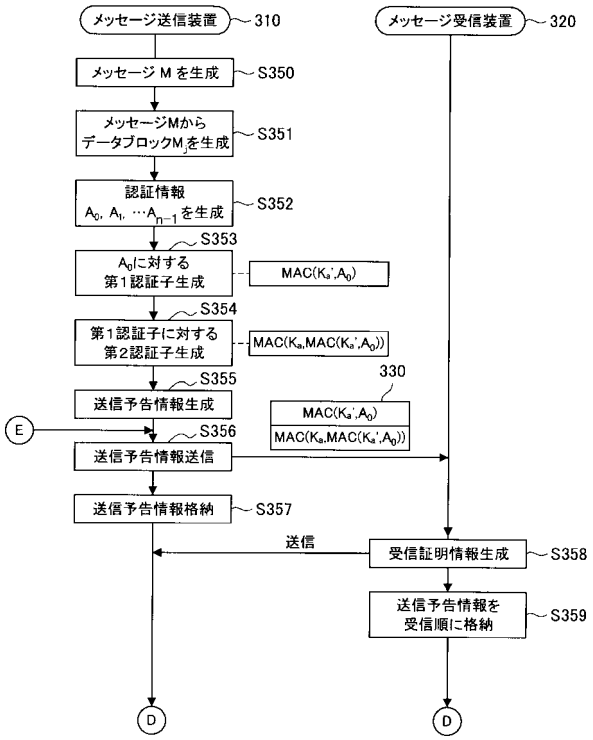
【図２１】



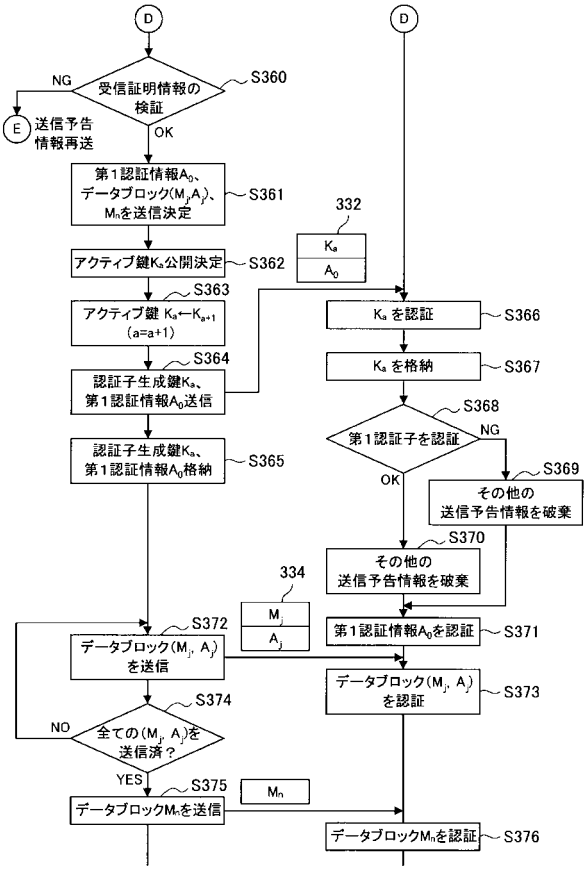
【図２２】



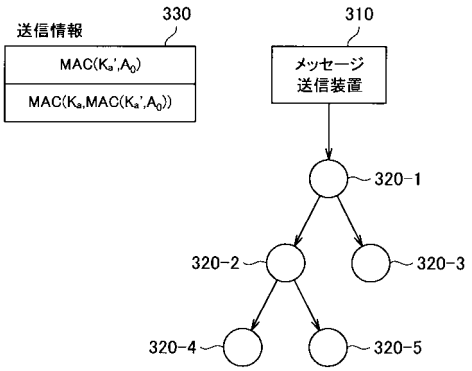
【図２３】



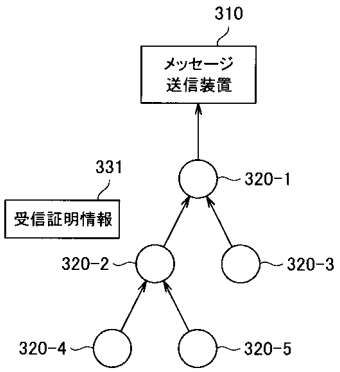
【図２４】



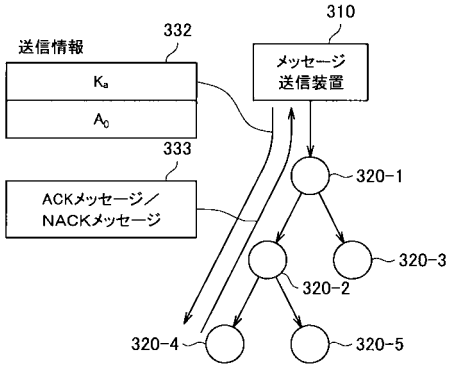
【図２５】



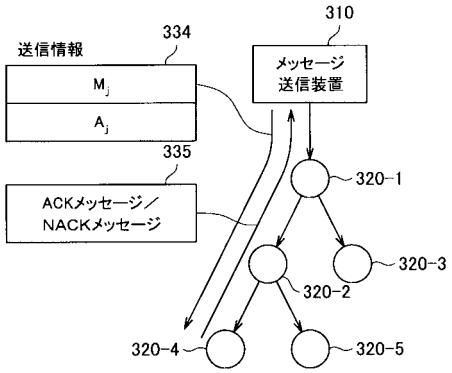
【図２６】



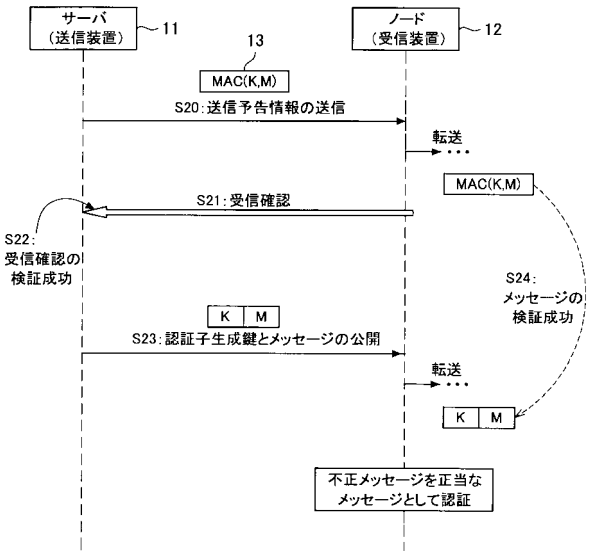
【図２７】



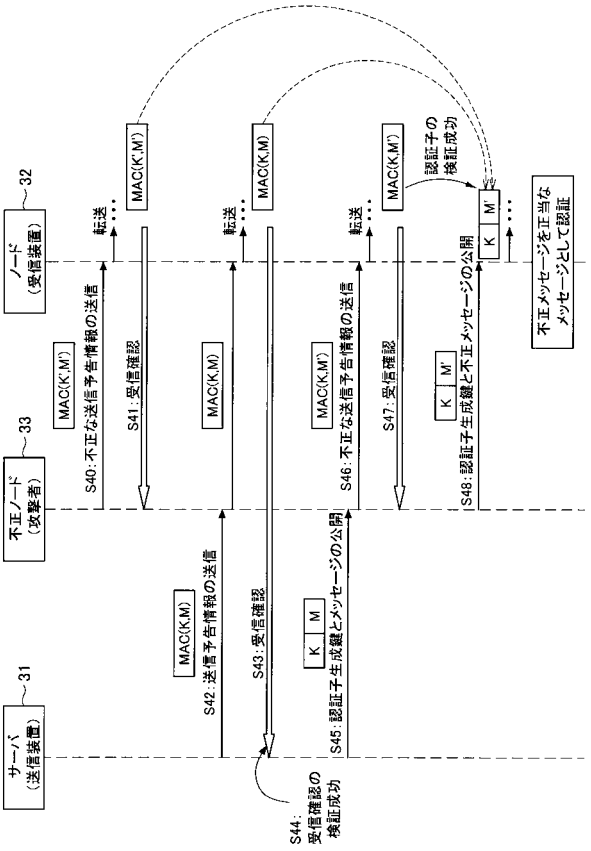
【図２８】



【図２９】



【図３０】


サーバ
（送信装置）
31
不正ノード
（攻撃者）
33
ノード
（受信装置）
32
MAC(K,M)
S42：送信予告情報の送信
S43：受信確認
S44：
受信確認の
検証成功
K
M
S45：認証子生成鍵とメッセージの公開
MAC(K',M')
S40：不正な送信予告情報の送信
S41：受信確認
転送
MAC(K,M)
転送
MAC(K',M')
S46：不正な送信予告情報の送信
S47：受信確認
転送
MAC(K,M')
認証子の
検証成功
K
M'
S48：認証子生成鍵と不正メッセージの公開
K
M'
不正メッセージを正当な
メッセージとして認証

フロントページの続き

(56)参考文献 特開２００６－８１０８２（ＪＰ，Ａ）
米国特許出願公開第２００７／６７６３１（ＵＳ，Ａ１）
岡崎直宣，玉里梨香，“センサネットワークにおけるメッセージ認証方式の提案”，Memoirs of the Faculty of Engineering，Miyazaki University，日本，宮崎大学工学部，２００７年 ８月３０日，第３６巻，ｐ．２６５－２７２，ＵＲＬ，http://ir.lib.miyazaki-u.ac.jp/dspace/handle/123456789/868/
Takatsugu Yao，Shigeru Fukunaga，and Toshihisa Nakai，“Reliable Broadcast Massage Authentication in Wireless Sensor Networks”，LNCS，２００６年 9月１１日，Vol.4097，p.271-280
八百健嗣，福永茂，“センサネットワークにおける高信頼ブロードキャストメッセージ認証技術”，沖テクニカルレビュー，２００５年１０月，第２０４号，Ｖｏｌ．７２，Ｎｏ．４，ｐ．４０－４３，ＵＲＬ，http://www.oki.com/jp/Home/JIS/Books/KENKAI/n204/pdf/204_R11.pdf
八百健嗣，松村靖子，福永茂，“センサネットワークにおける高信頼ブロードキャストメッセージ認証方式”，情報処理学会研究報告，２００５－ＤＰＳ－１２２，２００５－ＣＳＥＣ－２８，日本，社団法人情報処理学会，２００５年 3月２２日，Ｖｏｌ．２００５，Ｎｏ．３３，ｐ．２４１－２４６
八百健嗣，川本康貴，松村靖子，福永茂，“センサネットワークのマルチホップツリー構造に適したセキュアな受信確認方式”，情報処理学会研究報告，２００４－ＭＢＬ－３０，日本，社団法人情報処理学会，２００４年 9月１７日，Ｖｏｌ．２００４，Ｎｏ．９５，ｐ．６９－７５

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２