(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5612006号
(P5612006)
(45)発行日　平成26年10月22日(2014.10.22)　(24)登録日　平成26年9月12日(2014.9.12)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 6　(全 14 頁)

(21)出願番号　特願2012-55603(P2012-55603)
(22)出願日　平成24年3月13日(2012.3.13)
(65)公開番号　特開2013-191962(P2013-191962A)
(43)公開日　平成25年9月26日(2013.9.26)
審査請求日　平成26年2月3日(2014.2.3)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100103263
弁理士　川崎　康
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100118843
弁理士　赤岡　明
(74)代理人　100144967
弁理士　重野　隆之

最終頁に続く

(54)【発明の名称】データ送信装置、データ受信装置、及びプログラム

(57)【特許請求の範囲】
【請求項１】
データパケットを生成するパケット生成部と、
自装置の時刻を計測する第１時計と、前記データパケットの送信先となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を格納する格納部と、
前記第１時計により計測された自装置の現在時刻に所定時間を加算して第１時刻を求め、前記精度情報を用いて前記第１時刻を修正して第２時刻を求め、求められた第２時刻、前記データパケット、及び所定の秘密鍵を用いて認証子を生成する認証子生成部と、
前記第２時刻に所定時間を加算した第３時刻に、前記認証子が付加された前記データパケットを前記他装置へ送信する通信部と、
を備え、
前記認証子生成部は、前記第１時計により計測された自装置の現在時刻に、前記認証子生成部が前記認証子の生成処理に要する時間と、前記通信部がデータ送信処理に要する時間とを加算して前記第１時刻を求めるデータ送信装置。
【請求項２】
認証子が付加されたデータパケットを受信する通信部と、
自装置の時刻を計測する第１時計と、前記データパケットの送信元となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を格納する格納部と、
前記データパケットの受信時刻から所定時間を減じて第１時刻を求め、前記精度情報を用いて前記第１時刻を修正して第２時刻を求め、求められた第２時刻、前記データパケッ

ト及び所定の鍵を用いて検証用認証子を生成し、前記データパケットに付加された認証子と前記検証用認証子とが一致するか否か判定する検証部と、
を備え、
前記検証部は、前記データパケットの通信時間の変化に応じて、前記所定時間又は前記精度情報を変更するデータ受信装置。
【請求項３】
自装置の時刻を計測する第１時計と、データパケットの送信先となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を格納する格納部と、
前記第１時計により計測された自装置の現在時刻に所定時間を加算して第１時刻を求め、前記精度情報を用いて前記第１時刻を修正して第２時刻を求め、求められた第２時刻、前記データパケット、及び所定の秘密鍵を用いて認証子を生成する認証子生成部と、
前記第２時刻に所定時間を加算した第３時刻に、前記認証子が付加された前記データパケットを前記他装置へ送信する通信部と、
を備え、
前記認証子生成部は、前記第１時計により計測された自装置の現在時刻に、前記認証子生成部が前記認証子の生成処理に要する時間と、前記通信部がデータ送信処理に要する時間とを加算して前記第１時刻を求めるデータ送信装置。
【請求項４】
データパケットを生成するステップと、
自装置の時刻を計測する第１時計により計測された自装置の現在時刻に所定時間を加算して第１時刻を求めるステップと、
前記第１時計と、前記データパケットの送信先となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を用いて、前記第１時刻を修正して第２時刻を求めるステップと、
前記第２時刻、前記データパケット、及び所定の秘密鍵を用いて認証子を生成するステップと、
前記第２時刻に所定時間を加算した第３時刻に、前記認証子が付加された前記データパケットを前記他装置へ送信するステップと、
をコンピュータに実行させるプログラムであって、
前記第１時刻を求めるステップは、前記第１時計により計測された自装置の現在時刻に、前記認証子の生成処理に要する時間と、前記通信部がデータ送信処理に要する時間とを加算して前記第１時刻を求めるプログラム。
【請求項５】
認証子が付加されたデータパケットを受信するステップと、
前記データパケットの受信時刻から所定時間を減じて第１時刻を求めるステップと、
自装置の時刻を計測する第１時計と、前記データパケットの送信元となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を用いて、前記第１時刻を修正して第２時刻を求めるステップと、
前記第２時刻、前記データパケット、及び所定の鍵を用いて検証用認証子を生成するステップと、
前記データパケットに付加された認証子と前記検証用認証子とが一致するか否か判定するステップと、
をコンピュータに実行させるプログラムであって、
前記データパケットの通信時間の変化に応じて、前記所定時間又は前記精度情報を変更するプログラム。
【請求項６】
自装置の時刻を計測する第１時計により計測された自装置の現在時刻に所定時間を加算して第１時刻を求めるステップと、
前記第１時計と、データパケットの送信先となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を用いて、前記第１時刻を修正して第２時刻を求めるステッ

プと、
前記第２時刻、前記データパケット、及び所定の秘密鍵を用いて認証子を生成するステップと、
前記第２時刻に所定時間を加算した第３時刻に、前記認証子が付加された前記データパケットを前記他装置へ送信するステップと、
をコンピュータに実行させるプログラムであって、
前記第１時刻を求めるステップは、前記第１時計により計測された自装置の現在時刻に、前記認証子の生成処理に要する時間と、前記通信部がデータ送信処理に要する時間とを加算して前記第１時刻を求めるプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、データ送信装置、データ受信装置、及びプログラムに関する。
【背景技術】
【０００２】
ネットワーク機器同士がデータ通信するにあたり、通信相手が正当なものであるか否かを判定するための機器認証が行われる。例えば、送信機器は、送信機器しか知り得ない秘密の鍵を用いてデータパケットを作成して送信する。受信機器は、受信機器の持つ秘密の鍵または公開の鍵を用いて、受信したデータパケットが送信機器により作成されたものであるか否かを判定する。機器認証の手法としては、共有鍵を用いてデータのハッシュ値を求め、これを認証子とするｈｍａｃや、公開鍵暗号を用いてデータに署名を付けるものが知られている。
【０００３】
このような鍵を用いてデータパケットを作成する手法では、受信したデータパケットが送信機器により作成されたものであることは判定できるが、通信途上において第三者に盗聴されてデータの到着が遅れたことや、全く同じデータが第三者により時間をずらして繰り返し送信（リプレイ・アタック）されたことを発見できなかった。
【０００４】
そのため、鍵だけではなく時刻情報も含めてデータパケットを作成することが行われている。このことにより、第三者がデータパケットに記録されている時刻情報を改ざんしようとしても、鍵を知っている正当な送信機器でないと正しい認証子を作成できないため、前述したリプレイ・アタック等の不正が行われることを防ぐことができる。
【０００５】
しかし、全てのデータパケットに時刻情報を格納すると、データ量が大きくなり、通信速度が遅くなったり、処理メモリ量が増大したりするという問題があった。
【０００６】
リプレイ・アタック等の不正を防止するために、時刻情報を各パケットに格納するのではなく、通信機器間で完全に時刻が一致する正確な時計を持ち、その時計の時刻に基づいて通信を行うという手法も考えられるが、完全に時刻が一致する高精度な時計を実装することは困難である。
【先行技術文献】
【非特許文献】
【０００７】
【非特許文献１】HMAC: Keyed-Hashing for Message Authentication (H. Krawczyk 他 1997/2 RFC2104)
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明は、高精度な時計を利用することなく、時刻を用いた機器認証を行うことができるデータ送信装置、データ受信装置、及び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】
【０００９】
本実施形態によれば、データ送信装置は、データパケットを生成するパケット生成部と、自装置の時刻を計測する第１時計と、前記データパケットの送信先となる他装置の時刻を計測する第２時計との同期の精度に基づく精度情報を格納する格納部と、前記第１時計により計測された自装置の現在時刻に所定時間を加算して第１時刻を求め、前記精度情報を用いて前記第１時刻を修正して第２時刻を求め、求められた第２時刻、前記データパケット、及び所定の秘密鍵を用いて認証子を生成する認証子生成部と、前記第２時刻に所定時間を加算した第３時刻に、前記認証子が付加された前記データパケットを前記他装置へ送信する通信部と、を備える。
【図面の簡単な説明】
【００１０】
【図１】スマートグリッドの構成の一例を示す図である。
【図２】第１の実施形態に係るデータ通信システムの概略構成図である。
【図３】第１の実施形態に係るデータ送信装置の概略構成図である。
【図４】第１の実施形態に係るデータ受信装置の概略構成図である。
【図５】第２の実施形態に係るデータ通信システムの概略構成図である。
【図６】第４の実施形態に係るデータ通信システムの概略構成図である。
【発明を実施するための形態】
【００１１】
以下、本発明の実施の形態を図面に基づいて説明する。
【００１２】
（第１の実施形態）図１は、第１の実施形態に係る機器認証方法が用いられる次世代電力通信網（スマートグリッド）の構成の一例を示しており、スマートグリッドを構成する各機器は、インターネット等の公衆ネットワークを介して通信可能に接続されている。
【００１３】
スマートグリッドでは、電力使用量を集計するスマートメータ３０１０ａと、家電機器を管理するホームサーバであるＨＥＭＳ（Home Energy Management System）３０２０が各家庭に設置される。また、商業ビルには、電力使用量を集計するスマートメータ３０１０ａと、ビル内の電気機器を管理するサーバであるＢＥＭＳ（Building Energy Management System）３０３０が設置される。
【００１４】
スマートメータ３０１０ａ、３０１０ｂは、コンセントレータ（中継器）３０４０によって数台ごとにまとめられ、通信網を介してメータデータ管理システムであるＭＤＭＳ（Meter Data Management System）３０５０と通信する。ＭＤＭＳ３０５０は、各家庭やビルのスマートメータ３０１０ａ、３０１０ｂから、一定の間隔で電力使用量を受信して記憶する。エネルギー管理システムであるＥＭＳ（Energy Management System）３０６０は、ＭＤＭＳ３０５０に集まった複数の家庭やビルの電力使用量、或いは、電力系統に設置されたセンサからの情報に基づいて、スマートメータ３０１０ａ、３０１０ｂ、ＨＥＭＳ３０２０、ＢＥＭＳ３０３０などに対して、電力使用を抑制するよう要求するなどの電力制御を行う。
【００１５】
また、ＥＭＳ３０６０は、遠隔端末ユニットであるＲＴＵ（Remote Terminal Unit）３０７１に接続された太陽光発電や風力発電などの分散電源３０８０、ＲＴＵ３０７２に接続された蓄電装置３０９０、及びＲＴＵ３０７３に接続された発電側との間の送電量を制御する送配電制御装置３１００を制御し、電力系統網全体の電圧および周波数を安定化させる。
【００１６】
図１に示すように、スマートグリッドでは、多種多様な機器がネットワークを介して接続されており、その多くは電力系統網の制御に関わるため、不正なデータ送信を防ぐ必要

があり、全てのデータについて認証を行うことが求められる。本実施形態に係る機器認証方法は、スマートグリッドを構成する任意の機器間のデータ認証に用いることができる。

【００１７】

例えば、家庭のスマートメータ３０１０ａがデータを送信し、ＭＤＭＳ３０５０がデータを受信する場合、データ送出クライアントであるスマートメータ３０１０ａ及びデータ受信サーバであるＭＤＭＳ３０５０が本実施形態に係る機器認証方法を用いて機器認証を行う。

【００１８】

図２は、スマートメータ３０１０ａが、ネットワーク回線（インターネット等）を使い、コンセントレータ３０４０を経由してＭＤＭＳ３０５０へデータパケットを送信する例を簡略的に示している。

【００１９】

データ送信クライアントであるスマートメータ３０１０ａは、事前に秘密鍵４００１ａを取得し、格納している。また、データ受信サーバであるＭＤＭＳ３０５０は、事前に検証用鍵４００１ｂを取得し、格納している。秘密鍵４００１ａと検証用鍵４００１ｂは暗号技術的に対になったものである。例えば、共通鍵を用いた認証を行う際には秘密鍵４００１ａと検証用鍵４００１ｂは同一の値を持つ。あるいはまた、公開鍵を用いた認証を行う際には、秘密鍵４００１ａと検証用鍵４００１ｂとは公開鍵暗号方式における秘密鍵と公開鍵の関係にある。秘密鍵４００１ａと検証用鍵４００１ｂとが暗号理論的に対になっていれば、それらはどのようなものであっても良い。

【００２０】

スマートメータ３０１０ａは、自装置の時刻を計測するクライアント時計４０１１を有しており、パケットの送信にあたっては、秘密鍵４００１ａおよびクライアント時計４０１１の示す時刻情報を用いて認証用の情報（認証子）を作成し、この認証子をパケットに付加して送信する。具体的には、例えば、送信すべきデータ、秘密鍵４００１ａ、及びクライアント時計４０１１の時刻情報を、ハッシュ関数の入力とし、ハッシュ関数の出力（ハッシュ値）を当該パケットの認証子としてパケットに付加して送信する。パケット送信の際、秘密鍵４００１ａおよび時刻情報は送信されない。

【００２１】

ＭＤＭＳ３０５０は、自装置の時刻を計測するサーバ時計４０１２を有しており、パケットの受信にあたっては秘密鍵４００１ｂおよびサーバ時計４０１２の示す時刻情報を用いて、受信したパケットに含まれている認証子が正しいものであるか否かを検証する。具体的には、例えば、受信したデータ、秘密鍵４００１ｂ、サーバ時計４０１２の時刻情報を、ハッシュ関数の入力とし、ハッシュ関数の出力（ハッシュ値）が当該パケットに付加されている認証子と一致すれば、正当な機器（スマートメータ３０１０ａ）から送信されたパケットであると判断する。ハッシュ値が認証子と一致しない場合は、不正なパケットと判断して受信パケットを廃棄するか、不正なパケットであるものとしてエラーを意味する返答を返す。

【００２２】

上述したハッシュ関数を用いる例においては、秘密鍵４００１ａと秘密鍵４００１ｂは共通の鍵であるとして説明したが、認証の方法はこれに限定するものではない。例えば公開鍵暗号を用いた署名およびその検証の方法は広く使われているが、それらについては既存の技術の組み合わせで容易に実現できるので、詳しい説明は省略する。

【００２３】

本実施形態では、スマートメータ３０１０ａが認証子を生成するにあたりクライアント時計４０１１の時刻情報を用い、ＭＤＭＳ３０５０が認証子を検証するにあたりサーバ時計４０１２の時刻情報を用いる。しかし、一般にクライアント時計４０１１の時刻とサーバ時計４０１２の時刻は完全には一致せず微妙なズレがあり、ズレのある時刻をそのまま使用して認証子の計算を行うと、正しい結果を得ることができない。このような問題を解決するための本実施形態による時刻の取扱い方法については後述する。

【００２４】
なお、ここで説明したクライアント時計４０１１およびサーバ時計４０１２は、いずれも時刻が概ね正しいものであることを前提としている。この前提が成り立つためには、例えば正確な水晶発振器等を用いた精度の高い時計を用いることもできるが、一般的には、図２に示すような、時刻の同期を取るための時刻サーバ３５０１が設けられる。クライアント時計４０１１及びサーバ時計４０１２のうち少なくともいずれか一方は、時刻サーバ３５０１から現在時刻の情報を随時受信することで、概ね正しい時刻情報を持つことができる。
【００２５】
時刻サーバ３５０１は例えばＧＰＳ衛星であり、スマートメータ３０１０ａおよびＭＤＭＳ３０５０は時刻情報を無線によって受信し、時刻情報をそれぞれクライアント時計４０１１およびサーバ時計４０１２に伝達する。あるいはまた、時刻サーバ３５０１がインターネットを介してスマートメータ３０１０ａ、ＭＤＭＳ３０５０と通信し、ＮＴＰ（Network Time Protocol）などの方法で時計の同期を行うことも可能である。時計の同期の方法は限定されない。また、図２に示す例では、時刻サーバ３５０１は１つ設けているが、複数の時刻サーバを設けて、より正確な情報が得られるようにしてもよい。
【００２６】
また、何等かの方法により、予めクライアント時計４０１１とサーバ時計４０１２の時刻を合わせておき、その後の誤差が問題にならない場合は、時刻サーバ３５０１が不要であることは言うまでもない。
【００２７】
なお、本実施形態では、コンセントレータ３０４０はパケットを転送するだけの機能しか持たないものとし、認証子の検証などは行わないものとしているが、もちろん、コンセントレータ３０４０が本実施形態に係る機器認証方法を実行できるようにしてもよい。
【００２８】
図３に、スマートメータ３０１０ａに設けられるデータ送信装置の概略構成を示す。データ送信装置は、パケット生成部３０１、認証子生成部３０２、通信部３０３、精度情報格納部３０５、及び送信修正値格納部３０６を備えている。パケット生成部３０１は、送信するデータパケットを生成する。インターネット上で通信を行う場合、通常はＩＰ（Internet Protocol）通信が用いられるため、パケット生成部３０１はＩＰパケットを生成する。これは一般的な通信機器が持つ機能であるため、詳細な説明は省略する。
【００２９】
認証子生成部３０２は、ＩＰパケットのヘッダ部分に記載されている送信先ＩＰアドレスを参照し、送信先機器がＭＤＭＳ３０５０であると判断したら、秘密鍵４００１ａを用いて認証子を生成する。この例では、送信先がＭＤＭＳ３０５０である場合のみについて説明するため、使用される鍵は秘密鍵４００１ａのみであるが、データ送信先が複数ある場合には、送信先毎に異なる鍵を用いることもできる。その場合、データ送信装置には、送信先機器と、各機器向けの認証子を作成するための秘密鍵とを対応付けたテーブルを記憶する記憶部が設けられ、認証子生成部３０２は、テーブルを参照して、送信先機器に対応する秘密鍵を取り出す。
【００３０】
認証子生成部３０２は秘密鍵４００１ａと、クライアント時計４０１１の現在値（現在時刻）を修正した値を用いて、送信パケットに対応する認証子を生成する。クライアント時計４０１１の現在値の修正方法は後述する。
【００３１】
認証子を生成するアルゴリズムについては従来から知られているさまざまな方式を用いることができ、特に限定されない。例えば、ｈｍａｃ方式を用い、パケットのデータとクライアント時計４０１１の現在値を修正した値を入力として、秘密鍵４００１ａによる鍵付きハッシュ計算を行い、認証子を生成する。ｈｍａｃ方式では入力であるデータと鍵が同一であれば、常に同一の認証子が生成されるため、時刻も入力に用いることで、パケッ

トのデータ同一であっても、時刻が異なれば異なる認証子が生成されるようにして、安全性が高められている。

【００３２】

本実施形態では、認証子の生成に際して、クライアント時計４０１１の現在時刻Ｔ０をそのまま用いるのではなく、以下の手順で修正した値が用いられる。

【００３３】

まず、認証子生成部３０２が、時刻Ｔ０を、実際にパケットが送信される時刻付近の時刻Ｔ１に修正する。例えば、認証子生成部３０２がパケット生成部３０１からパケットを受け取ってから、パケットが実際に通信部３０３からＭＤＭＳ３０５０へ送信されるまでに要する処理時間を時刻Ｔ０に加算して、時刻Ｔ１が求められる。さらに、通信部３０３がパケットを送信してから、ＭＤＭＳ３０５０が実際にパケットを受信するまでに要する通信時間を加算して時刻Ｔ１を求めても良い。

【００３４】

次に、認証子生成部３０２は、精度情報格納部３０５に格納されている精度情報を用いて時刻Ｔ１を丸めて（端数処理して）時刻Ｔ２を生成する。例えば、図２に示すシステムにおいて、クライアント時計の信頼性が５秒程度の精度である場合、１秒単位の時刻を用いても、スマートメータ３０１０ａとＭＤＭＳ３０５０とで同じ時刻を共有することは困難である。そのため、時刻Ｔ１を、例えば２０秒単位の精度に丸めて、時刻Ｔ２を得る。

【００３５】

精度情報格納部３０５は、精度情報を格納する。精度情報は、この丸める単位の情報であり、これは予め決められているものとする。例えば、本実施形態では「２０秒」という値に相当する。

【００３６】

認証子生成部３０２は、このような手順によって得られた時刻Ｔ２を用いて認証子を生成し、生成した認証子をＩＰパケット内に付加する。認証子を付加する方法は既存のＩＰ（インタネット・プロトコル）仕様に準拠することが望ましく、例えばＩＰヘッダのオプション部のデータとして認証子を格納する。ＴＣＰヘッダのオプション部や、ＴＣＰ／ＤＹＮなどのデータを持たないＴＣＰヘッダのデータ部などに認証子を格納してもよい。また、近年の拡張されたＩＰｓｅｃプロトコルにおけるＡＨ（Authentication Header）も認証子格納フィールドに相当する。

【００３７】

通信部３０３は、上述したような方法で認証子が付加されたパケットを、コンセントレータ３０４０を経由して、サーバであるＭＤＭＳ３０５０に向けて送信する。

【００３８】

このような手順によれば、認証子の計算には２０秒単位に丸めた値が用いられるため、例えば ９時８分１８秒頃送信されたパケットは、２０秒単位に丸めた値である９時８分２０秒を用いて認証子が計算されたことになる。ＭＤＭＳ３０５０のサーバ時計４０１２が多少ズレており、例えばＭＤＭＳ３０５０が９時８分２５秒にパケットを受信したとしても、受信時刻を丸めた値は送信側と同じ９時８分２０秒となり、一致する。そのため、ＭＤＭＳ３０５０が、サーバ時計４０１２の示す時刻を用いて計算した値（例えば、ハッシュ値）が、パケットに付加されている認証子と一致するか否かで、パケットの認証を行うことができる。

【００３９】

ただし、この方法では、時間の境界線が明確でない。例えば９時８分３０秒頃送信されたパケットに用いられた時刻Ｔ２が、９時８分２０秒であるのか、又は９時８分４０秒であるのか明確でない。このため、送信側が認証子の生成に用いた時間と、受信側がパケット認証のために用いた時間とが異なる可能性が高くなる。

【００４０】

このような時間のずれを防ぐために、例えば、時刻Ｔ２を用いて２０秒単位でパケットを送信することで、ＭＤＭＳ３０５０は、９時８分２０秒前後と９時８分４０秒前後にパ

ケットを受信することが多くなり、９時８分３０秒（境界）前後の紛らわしい時間帯にパケットを受信する可能性は低くなる。

【００４１】

しかし、この方法では、全てのパケットが２０秒おきにしか送信できないこととなり、通信の負荷が集中し、実際に通信可能なネットワークの性能よりも小さい量のデータしか通信できなくなり、好ましくない。

【００４２】

そこで、本実施形態では、時刻Ｔ２に事前に決めた送信修正値を加えた時刻Ｔ３に当該パケットを送信する。通信部３０３は、認証子の付加されたパケットを直ちに送信するのではなく、送信修正値格納部３０６に予め記憶された送信修正値を時刻Ｔ２に加えた時刻Ｔ３まで待ってから、送信する。時刻Ｔ２は認証子生成部３０２が計算した値である。例えば、認証子の生成に用いた時刻Ｔ２が９時８分２０秒であり、送信修正値格納部３０６に格納されている送信修正値が１２秒の場合、通信部３０３は９時８分３２秒に送信を行う。

【００４３】

このようにしてスマートメータ３０１０ａから送信された認証子付きパケットが、ＭＤＭＳ３０５０によって受信される。

【００４４】

図４に、ＭＤＭＳ３０５０に設けられるデータ受信装置の概略構成を示す。データ受信装置は、パケット処理部３５１、認証子検証部３５２、通信部３５３、精度情報格納部３５５、及び受信修正値格納部３５６を備えている。

【００４５】

通信部３５３は、スマートメータ３０１０ａから送信された認証子付きパケットを受信し、その受信時刻Ｔ４を記録した上で、認証子検証部３５２にパケットと受信時刻Ｔ４を渡す。認証子検証部３５２が通信部３５３からパケットを受け取った時刻を受信時刻Ｔ４としてもよい。

【００４６】

例えば、スマートメータ３０１０ａからパケットが送信された時刻は、クライアント時計４０１１の時刻で９時８分３２秒である。スマートメータ３０１０ａからＭＤＭＳ３０５０までの通信に２秒掛かったとすると、受信時刻Ｔ４は、９時８分３４秒にサーバ時計４０１２とクライアント時計４０１１の誤差分を加えたものとなる。例えば、サーバ時計４０１２の方がクライアント時計４０１１よりも５秒進んでいる場合、ＭＤＭＳ３０５０で計測される受信時刻Ｔ４は９時８分３９秒となる。

【００４７】

認証子検証部３５２は、スマートメータ３０１０ａ（送信機器側）と同様の演算を行い、検証用認証子を算出する。まず、認証子検証部３５２は、受信時刻Ｔ４から、受信修正値格納部３５６に予め格納してある受信修正値を減じた時刻Ｔ５を求める。受信修正値は、スマートメータ３０１０ａの送信修正値格納部３０６に格納されている送信修正値に、スマートメータ３０１０ａがパケットを送信してから、ＭＤＭＳ３０５０がパケットを受信するまでに要する通信時間を加えたものとする。例えば、送信修正値が１２秒、通信時間が１秒程度の場合、受信修正値は１３秒とする。もちろん、受信修正値は正確にこのような値に定める必要はなく、概ねこの程度の値としておけばよい。これにより、時刻Ｔ５は９時８分３９秒（＝受信時刻Ｔ４）から１３秒を減じた９時８分２６秒となる。

【００４８】

次に、認証子検証部３５２は、この時刻Ｔ５の値を、精度情報格納部３５５に予め格納してある精度情報（この例では２０秒）で丸めた（端数処理した）時刻Ｔ６を求める。そして、認証子検証部３５２は、時刻Ｔ６を用いて検証用認証子を算出する。例えば、時刻Ｔ５が９時８分２８秒、精度情報が２０秒である場合、時刻Ｔ６は９時８分２０秒となる。

【００４９】

このような手順により、受信側機器であるＭＤＭＳ３０５０の認証子検証部３５２は、送信側機器であるスマートメータ３０１０ａの認証子生成部３０２で認証子計算に用いられた時刻Ｔ２と一致する時刻Ｔ６を得ることができる。

【００５０】

認証子検証部３５２は、時刻Ｔ６、検証用鍵４００１ｂ、（認証子部分を除く）パケットのデータを用いて、送信側機器であるスマートメータ３０１０ａでの認証子生成と同じ演算を行い、検証用認証子を求める。ＭＤＭＳ３０５０が受信したパケットが正当なものであれば、同一の入力に対し同一の計算を行うのであるから算出される値も同一となる。そのため、算出した検証用認証子が、パケットに含まれている認証子と同一であるか否かにより、パケットの認証を行うことができる。すなわち、検証用認証子がパケットに含まれている認証子と同一であれば認証に成功したものとし、パケットがパケット処理部３５１に渡され、通常の処理、例えばアプリケーションの起動が行われる。一方、検証用認証子がパケットに含まれている認証子と異なる場合は、認証に失敗したものとし、パケット処理部３５１にはデータを渡すことなく処理を終了する。認証に失敗した場合は、認証エラーを表す何等かのデータをパケット処理部３５１または通信部３５３に渡してもよい。

【００５１】

このように、本実施形態によれば、パケットに時刻Ｔ２の値を格納する必要は無く、サーバ／クライアント間で時計が完全に一致している必要も無い。そのため、通信負荷を抑えた効率の良い通信を行うことができる。また、高精度な時計を利用することなく、時刻を用いた機器認証を正しく行うことができる。

【００５２】

本実施形態によれば、インターネットなどの通信回線で接続された性能や特性の異なる複数の通信機器が混在していたり、有線や無線など異なる性質の通信ネットワークが混在したりするスマートグリッド網において、機器間でデータ認証を行う際に、通信を行う機器（送信機器と受信機器）が事前に時計同期の精度情報、および秘密鍵を持ち、時計の時刻を修正し、時計精度に応じて丸めた値を、パケット認証子の生成／検証に用いる。これにより、通信する両者が時刻情報そのものをデータパケットに格納することなく、時刻を用いた機器認証を行うことができる。

【００５３】

なお、上記実施形態では、説明の便宜上、クライアント時計４０１１及びサーバ時計４０１２を何時何分何秒といった実際の時刻を示す時計としたが、異なる時刻において異なる認証子を生成する目的のカウンターであれば、どのような形態でも構わない。例えば、時計を、３秒に１回だけ進むカウンターとしてもよい。また、そのカウンターのカウント値が０となる起点はいつでも良い。また、用途によっては１年で元に戻るような簡易的なカウンターであっても構わない。もちろん、１年で元に戻るカウンターのみを使えば１年後に同じ認証子が生成されるが、その場合においても、時計以外の入力パラメータを認証子演算に用いることは容易である。

【００５４】

（第２の実施形態）上記第１の実施形態では、サーバであるＭＤＭＳ３０５０とクライアントであるスマートメータ３０１０ａを１台ずつとして説明したが、ＭＤＭＳ３０５０及び／又はスマートメータ３０１０ａが複数台あってもよい。

【００５５】

例えば、図５に示すように、２台のスマートメータ３０１０ａ、３０１０ｂと、１台のＭＤＭＳ３０５０とが設けられていてもよい。スマートメータ３０１０ａとスマートメータ３０１０ｂは同じ構成でも良いし、認証子の生成およびパケットの送出に関連するパラメータの少なくとも一部が異なるものであっても良い。具体的には、スマートメータ３０１０ａで使用される秘密鍵４００１ａと、スマートメータ３０１０ｂで使用される秘密鍵４００２ａとが異なるものでも良いし、精度情報や送信修正値が異なっていてもよい。ＭＤＭＳ３０５０は、スマートメータ３０１０ａ、３０１０ｂの各々に対応したパラメータを持つ。スマートメータ３０１０ａ、３０１０ｂとＭＤＭＳ３０５０の対（組み合わせ）

ごとに異なるパラメータとすることで、不正が困難になるという暗号理論的な安全性が高まる。また、以下のような利点が得られる。

【００５６】

時計の精度は全ての機器で同じとは限らない。例えば、時計の精度が２０秒程度の安価な機器と、時計の精度が１秒程度の高価な機器が混在している場合、精度が全て２０秒程度であるとしてシステムを設計すれば、精度が１秒程度の高価な機器においても、同一のデータパケットに対し同一の認証子が生成される時間帯が２０秒程度と長くなり、高価な機器に見合った安全性が実現できなくなるおそれがある。また、精度が全て１秒程度であるとしてシステムを設計すれば、精度が２０秒程度の安価な機器において、正当な通信の認証を失敗する確率が上がり、パケットの再送処理の増大などにより通信の効率が下がる可能性が高まる。しかし、機器毎に時計の精度を設定することにより、これらの問題は解決する。また、変更するのは予め決める精度情報の値のみで良く、それぞれに異なるソフトウェア開発を行う必要は無い。

【００５７】

さらに、精度情報および送信修正値が機器毎に異なることにより、パケットの送信時刻が集中することを防ぐことができる。

【００５８】

また、通信に要する時間も、ネットワーク構成の違いなどにより機器毎に異なる場合があり、機器毎にその調整パラメータ値も異なるはずであり、結果として受信修正値も異なるものに設定できた方が、より精度の高いパラメータ調整を行うことができる。

【００５９】

これらの特徴は、サーバであるＭＤＭＳ３０５０が複数ある場合や、サーバであるＭＤＭＳ３０５０とクライアントであるスマートメータがともに複数ある場合も同様である。

【００６０】

（第３の実施形態）上記実施形態においては、クライアント時計４０１１とサーバ時計４０１２の誤差の大きさや、パケット通信に要する時間の長さ及びばらつきによって、精度情報及び受信修正値を適切に設定する必要があるが、特定のスマートメータとＭＤＭＳ３０５０の間の通信時間は、ネットワークの混雑等の外的要因に依存するものであり、予め決定することはできない。したがって、通信時間のばらつきを考慮して、精度情報や受信修正値を決めることが好ましい。

【００６１】

例えば、９０％のケースにおいて通信時間は０．１秒から０．２秒の間であり、９９％のケースにおいて通信時間が０．１秒から０．３秒の間であった場合、受信修正値は送信修正値に０．３秒以上加算した値を用いることが好ましい。このように、通信パケットの受信に要する通信時間の分布を考慮して、受信修正値及び／又は精度情報を決定することが好ましい。

【００６２】

また、通信時間が随時変化するシステムもある。例えば、無線によりワン・ホップで到達できるケースでは、通信時間が０．３秒前後であり、無線のメッシュネットワークで、何段かの経由をして通信できるケースでは通信時間が最大０．９秒程度にまで伸びるといったケースが考えられる。そのような場合、最初から最大０．９秒程度であることを見込み１～２秒の余裕を持った設定をしても良いが、通信経路の切り替えが起こった際に随時パラメータを変更した方が、より正確な設定を行うことができ、その結果エラー再送などの確率を下げることができる。したがって、通信パケットの受信に要する通信時間の変化に応じて、受信修正値及び／又は精度情報を随時変更することが望ましい。トレースルートにより通信経路の切り替えを検出してもよいし、エラーが続く場合に通信経路が切り替わったと判断してもよい。

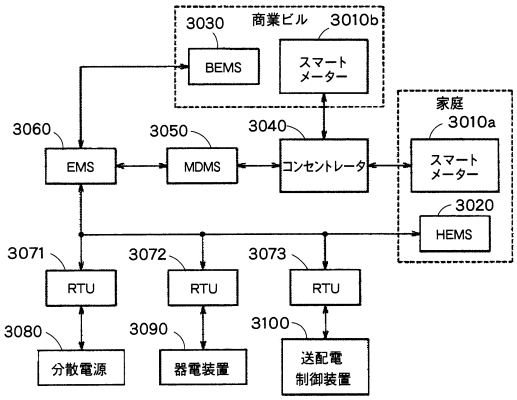
【００６３】

（第４の実施形態）図６に、第４の実施形態に係るデータ通信システムの概略構成を示す。図６は、図２に示すシステムに認証情報管理サーバ６０１を設けた構成となっている

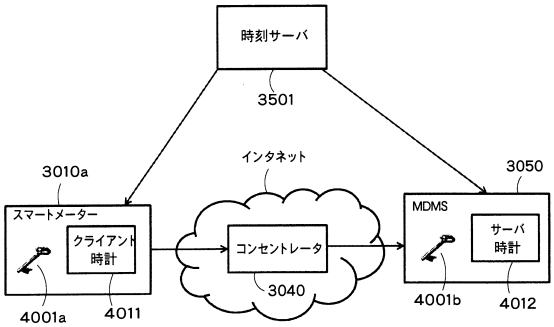
。
【００６４】
認証管理サーバ６０１は、送信側認証装置（スマートメータ３０１０ａ）と通信を行い、精度情報、秘密鍵、送信修正値等を指示することができる。また、認証管理サーバ６０１は、受信側認証装置（ＭＤＭＳ３０５０）と通信を行い、精度情報、検証用鍵、受信修正値等を指示することができる。
【００６５】
スマートメータ３０１０ａが用いるパラメータと、ＭＤＭＳ３０５０が用いるパラメータには依存関係があるため、それぞれ独立にパラメータ設定するのではなく、認証管理サーバ６０１が両者のパラメータを設定することが好ましい。
【００６６】
また、認証管理サーバ６０１は、新規にスマートメータを設置した際に、ＭＤＭＳ３０５０に対応する検証用鍵を通知してもよい。また、認証管理サーバ６０１は、スマートメータ３０１０ａ及びＭＤＭＳ３０５０に対して、定期的に新しい鍵を通知し、鍵を更新するようにしてもよい。
【００６７】
上記実施形態では、スマートグリッドにおける機器間のデータ認証について説明したが、図３、図４に示すデータ送信装置、データ受信装置は、時刻を用いた機器認証を行う通信システムに適用することができる。
【００６８】
上述した実施形態で説明したデータ送信装置及びデータ受信装置の少なくとも一部は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、データ送信装置及びデータ受信装置の少なくとも一部の機能を実現するプログラムをフレキシブルディスクやＣＤ－ＲＯＭ等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の着脱可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。
【００６９】
また、データ送信装置及びデータ受信装置の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。
【００７０】
なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。
【符号の説明】
【００７１】
３０１　パケット生成部
３０２　認証子生成部
３０３　通信部
３０５　精度情報格納部
３０６　送信修正値格納部
３５１　パケット処理部
３５２　認証子検証部
３５３　通信部
３５５　精度情報格納部
３５６　受信修正値格納部
３０１０ａ、ｂ　スマートメータ

３０５０　ＭＤＭＳ
４０１１　クライアント時計
４０１２　サーバ時計

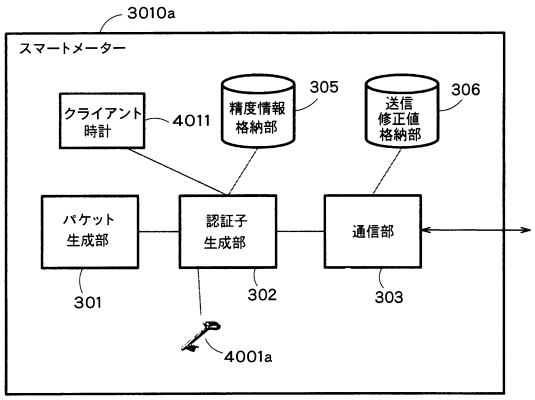
【図１】



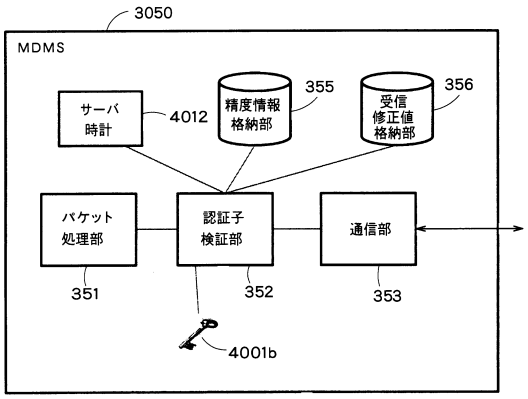
【図２】



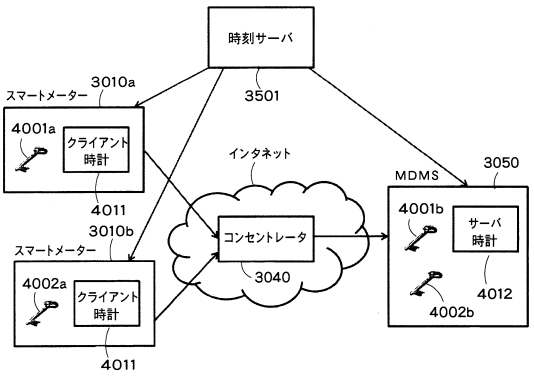
【図３】



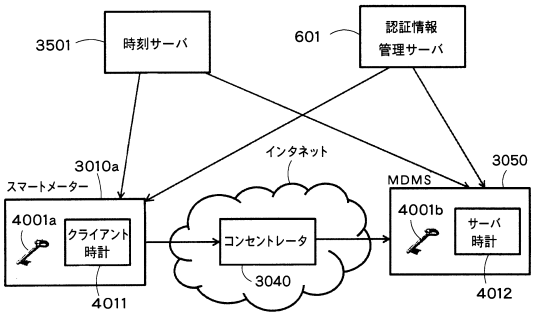
【図４】


3050
MDMS
サーバ
時計
4012
精度情報
格納部
355
受信
修正値
格納部
356
パケット
処理部
認証子
検証部
通信部
351
352
353
4001b

【図５】


時刻サーバ
3501
スマートメーター
3010a
4001a
クライアント
時計
4011
インタネット
MDMS
3050
4001b
サーバ
時計
4012
4002b
3010b
スマートメーター
4002a
クライアント
時計
4011
コンセントレータ
3040

【図６】


3501
時刻サーバ
601
認証情報
管理サーバ
インタネット
3010a
スマートメーター
3050
MDMS
4001a
クライアント
時計
コンセントレータ
4001b
サーバ
時計
3040
4011
4012

フロントページの続き

(72)発明者　高　橋　俊　成
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　三　宅　秀　享
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　打出　義尚

(56)参考文献　米国特許出願公開第２００３／０２０４７２８（ＵＳ，Ａ１）
特開平１１－３１６７４０（ＪＰ，Ａ）
国際公開第２００４／０１２４０８（WO，Ａ１）
特開２００２－０２４４２３（ＪＰ，Ａ）
特開２０１２－１９９８２０（ＪＰ，Ａ）
特開２０１２－１７５３５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００