(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5374752号
(P5374752)
(45)発行日　平成25年12月25日(2013.12.25)　(24)登録日　平成25年10月4日(2013.10.4)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04L 9/14 (2006.01)　　H04L 9/00 641

請求項の数 11　(全 22 頁)

(21)出願番号　特願2009-8823(P2009-8823)
(22)出願日　平成21年1月19日(2009.1.19)
(65)公開番号　特開2010-166486(P2010-166486A)
(43)公開日　平成22年7月29日(2010.7.29)
審査請求日　平成23年8月2日(2011.8.2)

(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
(73)特許権者　504182255
国立大学法人横浜国立大学
神奈川県横浜市保土ヶ谷区常盤台７９番１号
(74)代理人　100081961
弁理士　木内　光春
(72)発明者　片山　茂樹
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　関口　勝彦
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】保護制御計測システムと装置、およびデータ伝送方法

(57)【特許請求の範囲】
【請求項１】
電力系統の保護制御計測を行う保護制御計測装置を含む複数の装置を伝送路で接続し、これら複数の装置間でデータの授受を行う保護制御計測システムにおいて、
各装置は、
予め設定された設定数の鍵データを保存する鍵データ保存手段と、
送信目的の本体データと、前記鍵データ保存手段に保存された１つの鍵データとを使用して認証タグを生成する認証タグ生成手段と、
生成した認証タグをその生成に使用した本体データに付加して送信データとし、この送信データを前記伝送路に送信すると共に、前記伝送路からデータを受信して、この受信したデータを本体データと認証タグに分離する送受信手段と、
前記送受信手段により受信した受信データ中の本体データと認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの正当性を認証する受信データ認証手段を備え、
情報量的観点に基づくセキュリティ方式として、前記認証タグ生成手段によって認証タグを生成する際に使用する鍵データを毎回変更する方式が採用されると共に、個々の鍵データを、前記保護制御計測装置の運用期間に応じて予め設定された設定期間内において予め設定された鍵データの繰り返し使用回数の上限を超えて使用しないという使用回数制限が採用され、
前記設定期間内における前記送信目的の本体データの送信回数合計と前記鍵データの繰

り返し使用回数の上限に応じて前記鍵データの前記設定数が決定され、この鍵データの設定数に応じて鍵データサイズが決定されることによって、運用開始時点で、前記鍵データ保存手段には、各々が前記鍵データサイズを有する前記設定数の鍵データが保存されている
ことを特徴とする保護制御計測システム。
【請求項２】
前記鍵データ保存手段中に保存された前記設定数の鍵データは、固定的に与えられた共通の固定鍵行列と、当該設定数の使い捨て鍵ベクトルとに分離されており、
前記認証タグ生成手段は、本体データのベクトルをｘ、固定鍵行列をＵ、使い捨て鍵ベクトルをｖとした場合に、認証タグベクトルｙを、以下のベクトル演算で求める
ことを特徴とする請求項１に記載の保護制御計測システム。

$$y = xU + v$$

【請求項３】
前記受信データ認証手段により受信データが不正なデータであると判定した場合に、この受信データを破棄する手段と、不正判定結果をセキュリティ情報として記録する手段を有する
ことを特徴とする請求項１に記載の保護制御計測システム。
【請求項４】
前記鍵データ保存手段中には、前記設定数の鍵データと共に、個々の鍵データを一意に特定する同数の鍵識別情報が保存されており、
前記送受信手段は、生成された認証タグと共に、この認証タグの生成に使用した鍵データを特定する鍵識別情報を前記本体データに付加して送信データとするように構成され、
前記受信データ認証手段は、受信した受信データ中の鍵識別情報により特定される鍵データを使用して受信データの正当性を認証するように構成されている
ことを特徴とする請求項１に記載の保護制御計測システム。
【請求項５】
不正な受信データが誤って正当と認証される確率を決定するために、鍵データおよび認証タグ生成アルゴリズムを利用者に設定させる手段を備えた
ことを特徴とする請求項１に記載の保護制御計測システム。
【請求項６】
前記鍵データ保存手段、認証タグ生成手段、送受信手段、受信データ認証手段を備えた前記装置の構成を有する複数の電気所の保護リレー装置を伝送路で接続し、各保護リレー装置により保護対象の電流、電圧サンプリングデータを他電気所の保護リレー装置と相互に送受信して電流差動演算を行う電流差動保護システムを構成する場合に、
各保護リレー装置は、
前記サンプリングデータを送信する際には、前記認証タグ生成手段により、送信目的の当該サンプリングデータと前記鍵データ保存手段に保存された１つの鍵データとを使用して認証タグを生成し、前記送受信手段により、生成した認証タグをその生成に使用したサンプリングデータに付加して送信データとし、
前記送受信手段によりデータを受信した際には、前記データ認証手段により、受信した受信データに含まれるサンプリングデータと認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの認証を行い、正当な受信データである場合にのみそのサンプリングデータを使用して電流差動演算を行うように構成されている
ことを特徴とする請求項１に記載の保護制御計測システム。
【請求項７】
各保護リレー装置は、前記受信データ認証手段により受信データが不正なデータであると判定した場合に、この受信データの値を零として電流差動演算を行うように構成されている
ことを特徴とする請求項６に記載の保護制御計測システム。
【請求項８】

各保護リレー装置は、前記受信データ認証手段により受信データが不正なデータであると判定した場合に、遮断器へのトリップ指令をロックするように構成されている
ことを特徴とする請求項６に記載の保護制御計測システム。
【請求項９】
前記鍵データ保存手段、認証タグ生成手段、送受信手段、受信データ認証手段を備えた前記装置の構成を有する複数の制御装置を伝送路で接続し、各制御装置により制御用コンピュータまたは他の制御装置からの制御指令を受信して被制御機器を制御する変電所制御システムを構成する場合に、
各制御装置は、
請求項１に記載の鍵データ保存手段、認証タグ生成手段、送受信手段、受信データ認証手段を備えており、
前記制御指令を送信する際には、前記認証タグ生成手段により、送信目的の当該制御指令と前記鍵データ保存手段に保存された１つの鍵データとを使用して認証タグを生成し、前記送受信手段により、生成した認証タグをその生成に使用した制御指令に付加して送信データとし、
前記送受信手段によりデータを受信した際には、前記データ認証手段により、受信した受信データ中の制御指令と認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの認証を行い、正当な受信データである場合にのみその制御指令を使用して被制御機器を制御するように構成されている
ことを特徴とする請求項１に記載の保護制御計測システム。
【請求項１０】
電力系統の保護制御計測を行うと共に、伝送路で接続された他の装置との間でデータの授受を行う保護制御計測装置において、
予め設定された設定数の鍵データを保存する鍵データ保存手段と、
送信目的の本体データと、前記鍵データ保存手段に保存された１つの鍵データとを使用して認証タグを生成する認証タグ生成手段と、
生成した認証タグをその生成に使用した本体データに付加して送信データとし、この送信データを前記伝送路に送信すると共に、前記伝送路からデータを受信して、この受信したデータを本体データと認証タグに分離する送受信手段と、
前記送受信手段により受信した受信データ中の本体データと認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの正当性を認証する受信データ認証手段を備え、
情報量的観点に基づくセキュリティ方式として、前記認証タグ生成手段によって認証タグを生成する際に使用する鍵データを毎回変更する方式が採用されると共に、個々の鍵データを、前記保護制御計測装置の運用期間に応じて予め設定された設定期間内において予め設定された鍵データの繰り返し使用回数の上限を超えて使用しないという使用回数制限が採用され、
前記設定期間内における前記送信目的の本体データの送信回数合計と前記鍵データの繰り返し使用回数の上限に応じて前記鍵データの前記設定数が決定され、この鍵データの設定数に応じて鍵データサイズが決定されることによって、運用開始時点で、前記鍵データ保存手段には、各々が前記鍵データサイズを有する前記設定数の鍵データが保存されている
ことを特徴とする保護制御計測装置。
【請求項１１】
電力系統の保護制御計測を行うと共に、伝送路で接続された他の装置との間でデータの授受を行う保護制御計測装置のデータ伝送方法において、
前記保護制御計測装置は、予め設定された設定数の鍵データを保存する鍵データ保存手段を備え、
前記保護制御計測装置によって、
送信目的の本体データと、前記鍵データ保存手段に保存された１つの鍵データとを使用

して認証タグを生成する認証タグ生成処理と、
生成した認証タグをその生成に使用した本体データに付加して送信データとし、この送信データを前記伝送路に送信する送信処理と、
前記伝送路からデータを受信して、この受信したデータを本体データと認証タグに分離する受信処理と、
受信した受信データ中の本体データと認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの正当性を認証する受信データ認証処理を行い、
情報量的観点に基づくセキュリティ方式として、前記認証タグ生成処理によって認証タグを生成する際に使用する鍵データを毎回変更する方式が採用されると共に、個々の鍵データを、前記保護制御計測装置の運用期間に応じて予め設定された設定期間内において予め設定された鍵データの繰り返し使用回数の上限を超えて使用しないという使用回数制限が採用され、
前記設定期間内における前記送信目的の本体データの送信回数合計と前記鍵データの繰り返し使用回数の上限に応じて前記鍵データの前記設定数が決定され、この鍵データの設定数に応じて鍵データサイズが決定されることによって、運用開始時点で、前記鍵データ保存手段には、各々が前記鍵データサイズを有する前記設定数の鍵データが保存されている
ことを特徴とする保護制御計測装置のデータ伝送方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信ネットワークで接続された複数の装置からなるシステムに関するものであり、特に、電力系統の保護制御計測システムに関する。
【背景技術】
【０００２】
近年、保護制御計測システムにおいても、イーサネット（登録商標）やＴＣＰ／ＩＰなどの汎用ネットワーク技術を適用する例が増加している。この場合に必ず問題となるのが、サイバーセキュリティ対策である。電力用通信のセキュリティ技術については、ＳＨＡアルゴリズムを用いた認証方式が、非特許文献１で規定されている。
【０００３】
しかし、非特許文献１で規定しているＳＨＡ（Secure Hash Algorithm）などの、現在主流となっている各種のセキュリティアルゴリズムは、非特許文献２で記述されているように、計算量に基づいて安全性を保証するものである。したがって、将来的に、計算機の性能が向上したり、またはその問題を解くためのより高速な手法が発見されたりした場合には、計算量に基づくそれらのセキュリティアルゴリズムは、セキュリティ面で不安全になってしまい、別の安全なアルゴリズムに変更しなければならない。
【０００４】
【非特許文献１】IEC62351 “Power systems management and associated information exchange - Data and communications security”
【非特許文献２】D. R. Stinson,「暗号理論の基礎」(ISBN4-320-02820-1),（原著：”CRYPTOGRAPHY: Theory and Practice”）
【非特許文献３】C. E. Shannon, “Communication theory of secrecy systems”, Bell Systems Technical Journal, 28, 1949, 656-715.
【発明の開示】
【発明が解決しようとする課題】
【０００５】
一般的に、セキュリティ対策では、秘匿、認証、完全性の３つを考える必要があるが、保護制御計測システムは、そのミッションクリティカルな性格上、データの秘匿よりも認証が重要となる。また、伝送路は狭帯域の場合が多い。特に、複数の保護リレー装置間で相互にデータを送受信して電流差動演算を行うシステムにおいては、その動作性格上、認

証処理には高いリアルタイム性が要求される。さらに、保護制御計測システムは、長期間無停止で運用しなければならないケースが多く、装置内のアルゴリズム変更は容易にできないという制約がある。したがって、一般にＩＴ産業で用いられている計算量的観点によるセキュリティ技術を保護制御計測システムにそのまま適用することは、あまり適切ではない。

【０００６】

これに対して、非特許文献２には、シャノンの定理に基づく、情報量的観点によるセキュリティ技術が記載されており、情報量的セキュリティの理論的な研究は、非特許文献３がベースとなっている。このような情報量的セキュリティ技術としては、毎回鍵を変えてデータ送信を行うワンタイムパッド方式が知られている。このような情報量的セキュリティ技術は、通常の方式では、必要な鍵サイズが莫大になるので、電力系統の保護制御計測システムのような極めて高頻度でデータ授受を行う分野において実用化された例は殆ど報告されていない。

【０００７】

本発明は、上記のような従来技術の課題を解決するために提案されたものであり、その目的は、鍵データサイズが実用上実現できる範囲内に収まり、かつ、保護制御計測用として実装が容易な実用的な情報量的セキュリティ技術を構築し、そのような情報量的セキュリティ技術を使用した安全性・信頼性の高い保護制御計測システムと装置、およびデータ伝送方法を提供することである。

【課題を解決するための手段】

【０００８】

本発明は、電力系統の保護制御計測を行う保護制御計測装置を含む複数の装置を伝送路で接続し、これら複数の装置間でデータの授受を行う保護制御計測システムにおいて、各装置が、次のような技術的特徴を有するものである。すなわち、各装置は、予め設定された設定数の鍵データを保存する鍵データ保存手段と、送信目的の本体データと、前記鍵データ保存手段に保存された１つの鍵データとを使用して認証タグ(Authentication Tag)を生成する認証タグ生成手段と、生成した認証タグをその生成に使用した本体データに付加して送信データとし、この送信データを前記伝送路に送信すると共に、前記伝送路からデータを受信して、この受信したデータを本体データと認証タグに分離する送受信手段と、前記送受信手段により受信した受信データ中の本体データと認証タグ、および、前記鍵データ保存手段中に保存された鍵データを使用して受信データの正当性を認証する受信データ認証手段を備える。さらに、情報量的観点に基づくセキュリティ方式として、前記認証タグ生成手段によって認証タグを生成する際に使用する鍵データを毎回変更する方式が採用されると共に、個々の鍵データを、前記保護制御計測装置の運用期間に応じて予め設定された設定期間内において予め設定された鍵データの繰り返し使用回数の上限を超えて使用しないという使用回数制限が採用される。前記設定期間内における前記送信目的の本体データの送信回数合計と前記鍵データの繰り返し使用回数の上限に応じて前記鍵データの前記設定数が決定され、この鍵データの設定数に応じて鍵データサイズが決定されることによって、運用開始時点で、前記鍵データ保存手段には、各々が前記鍵データサイズを有する前記設定数の鍵データが保存されている。

【０００９】

このような特徴を有する本発明では、送信目的の本体データと、この本体データから生成された認証タグとを組み合わせてなるデータを送信し、受信側では受信したデータ中の本体データを元に生成した認証タグと、受信データ中に含まれている認証タグとを比較することで、伝送路上でのデータ改ざんの有無を検出できる。認証タグを生成する際に使用する鍵データは、データを送信する度に変更することで、計算量的観点ではなく情報量的観点からセキュリティを保証できる。

【００１０】

また、同じ鍵データを、設定期間内に設定回数以上使用しないという使用回数制限を採用したことで、保護制御計測装置の寿命から勘案した運用期間を設定期間とし、設定回数

を少なくすることにより、運用期間中における改ざん、なりすましの発生確率を極めて小さくできる。特に、設定期間という時間的制限を設けたことで、鍵データサイズを無限に大きくすることなく、保護制御装置の運用上で実現可能な程度の範囲内に鍵データサイズを収めることが可能となる。

【００１１】

また、本発明の保護制御計測装置とデータ伝送方法は、上記保護制御計測システムの特徴を、システムを構成する装置とそのデータ伝送方法の観点からそれぞれ把握したものである。

【発明の効果】

【００１２】

本発明によれば、鍵データサイズが実用上実現できる範囲内に収まり、かつ、保護制御計測用として実装が容易な実用的な情報量的セキュリティ技術を使用した、安全性・信頼性の高い保護制御計測システムと装置、およびデータ伝送方法を提供することができる。

【発明を実施するための最良の形態】

【００１３】

以下には、本発明の保護制御計測システムを適用した複数の実施形態について、図面を参照して具体的に説明する。

【００１４】

［第１の実施形態］

［システム構成］

図１は、本発明を適用した第１の実施形態に係る保護制御計測システムの構成を示すブロック図である。図１に示す保護制御計測システムは、同一構成の２台の保護制御計測装置１を伝送路２で接続して構成されている。伝送路２は、光ファイバ、マイクロ波、電力線などの各種の媒体から構成されている。保護制御計測装置１間で授受される具体的な送信目的データは、例えば、送電線両端子にて計測した送電線電流データ、あるいは遮断器遮断指令、変電所の機器状態などの各種の保護制御用データである。本明細書中では、このような送信目的の保護制御用データを「送信目的データ」または「（送信目的の）本体データ」と称している。

【００１５】

保護制御計測装置１は、送信目的データを取得する目的データ取得手段１１、予め設定された設定数の鍵データを保存する鍵データ保存手段１２、送信目的の本体データと鍵データとを使用して認証タグを生成する認証タグ生成手段１３、データを送受信する送受信手段１４、受信データの認証を行う受信データ認証手段１５を備えている。

【００１６】

本実施形態においては、本発明の特徴である情報量的観点に基づくセキュリティ方式として、次のような鍵データ使用方式を採用した認証タグ生成アルゴリズムを使用する。すなわち、一つには、認証タグ生成手段１３によって認証タグを生成する際に使用する鍵データ２２を毎回変更する方式が採用される。これに加えて、個々の鍵データ２２を、保護制御計測装置１の運用期間などの予め設定された設定期間内において予め設定された設定回数（例えば２回）以上は使用しないという使用回数制限が採用される。すなわち、使用回数制限における「設定回数」は、「鍵データの繰り返し使用禁止回数の下限の設定回数」であり、この回数が「２回」であれば、「鍵データの繰り返し使用回数の上限」は「１回」となる。

【００１７】

このような情報的観点に基づくセキュリティ方式を採用した認証タグ生成アルゴリズムを実現するために、２台の保護制御計測装置１の鍵データ保存手段１２には、完全同一の同数の鍵データからなる鍵データセットが保存されており、認証タグ生成手段１３、送受信手段１４、受信データ認証手段１５は、以下のような機能を有する。

【００１８】

認証タグ生成手段１３は、送信目的の本体データ２１と鍵データ２２とを使用して認証タグ２３を生成する機能に加えて、送受信手段１４から受信データ２４ａ中の本体データ２１ａを受け取った場合に、受信データ２４ａ中の認証タグ２３ａと比較するための認証タグ２３ｂを生成する機能を有する。この比較対照用の認証タグ２３ｂは、受信データ２４ａ中の本体データ２１ａと自装置内の鍵データ保存手段１２中に保存された鍵データ２２を使用して生成される。

【００１９】

送受信手段１４は、認証タグ生成手段１３によって生成した認証タグ２３をその生成に使用した本体データ２１に付加して送信データ２４とし、この送信データ２４を伝送路２に送信する機能と、伝送路２からデータ２４ａを受信して、この受信データ２４ａを本体データ２１ａと認証タグ２３ａに分離する機能を有する。

【００２０】

受信データ認証手段１５は、送受信手段１４により受信した受信データ２４ａ中の本体データ２１ａと認証タグ２３ａ、および、自装置内の鍵データ保存手段１２中に保存された鍵データ２２を使用して受信データの正当性の認証判定を行い、判定結果２５を出力する。この受信データ認証手段１５は、具体的には、受信データ２４ａ中の認証タグ２３ａと、認証タグ生成手段１３によって受信データ２４ａ中の本体データ２１ａと自装置内の鍵データ２２から生成された比較対照用の認証タグ２３ｂとを比較して、これらの認証タグ２３ａ，２３ｂが一致するか否かの判定を行い、判定結果２５を出力する。

【００２１】

なお、本明細書中および添付図面中において、受信側の本体データ、認証タグ、受信データを示す参照符号「２１ａ」、「２３ａ」、「２４ａ」中の符号「ａ」は、受信側の立場における受信データとそれに含まれるデータ（本体データと認証タグ）を送信側と区別するために使用している。また、受信データ中の本体データと自装置内の鍵データから生成された比較対照用の認証タグを示す参照符号「２３ａ」中の符号「ｂ」は、受信データ「２１ａ」中の認証タグ「２３ａ」と区別するために使用している。

【００２２】

［作用］

［システム動作］

図２は、図１に示した保護制御計測システムにおいて、一方の保護制御計測装置１（以下には、送信側装置１Ｔと称する）から、他方の保護制御計測装置１（以下には、受信側装置１Ｒと称する）に送信目的の本体データ２１を送信する場合の特徴的なデータ処理とデータの流れを示す図である。なお、この図２以降の、データ処理の特徴とデータの流れを示す各添付図面においては、簡略化の観点から、各装置１内の構成については、各実施形態における特徴的なデータ処理を行う手段のみを示している。

【００２３】

図２に示すように、送信側装置１Ｔにおいて、認証タグ生成手段１３に送信目的の本体データ２１が入力されると、認証タグ生成手段１３は、予め決められた鍵使用順序に従って選択される１つの鍵データ２２を読み込み、これらの本体データ２１と鍵データ２２から認証タグ２３を生成する。生成した認証タグ２３とその元となった本体データ２１は、送受信手段１４に入力される。送受信手段１４は、入力された本体データ２１と認証タグ２３を組み合わせて送信データ２４を生成し、この送信データ２４を、伝送路２を介して受信側装置１Ｒに送信する。

【００２４】

また、受信側装置１Ｒにおいて、送受信手段１４は、送信側装置１Ｔから送信されたデータ２４を受信データ２４ａとして受信する。ここで、送受信手段１４は、受信データ２４ａを本体データ２１ａと認証タグ２３ａに分離して、本体データ２１ａを認証タグ生成手段１３に、認証タグ２３ａを受信データ認証手段１５にそれぞれ入力する。認証タグ生成手段１３に受信データ２４ａ中の本体データ２１ａが入力されると、認証タグ生成手段１３は、自装置１Ｒ内の鍵データ２２を、予め決められた鍵使用順序に従って選択して読

み込み、これらの受信した本体データ２１ａと自装置内の鍵データ２２から比較対照用の認証タグ２３ｂを生成して受信データ認証手段１５に入力する。

【００２５】

受信データ認証手段１５は、入力された受信データ２４ａ中の認証タグ２３ａと比較対照用の認証タグ２３ｂとを比較して、これらの認証タグ２３ａ，２３ｂが一致するか否かの判定を行い、判定結果２５を出力する。

【００２６】

図３は、装置間で送信される送信データ２４のフォーマットを示す図である。この図３に示すように、送信データ２４は、物理層およびデータリンク層として付加されるヘッダとフッタに挟まれる形で、アプリケーション層として本体データと認証タグが加えられることにより構成されている。

【００２７】

［認証タグ生成アルゴリズム］

本実施形態において、情報量的観点に基づくセキュリティ方式を採用した認証タグ生成アルゴリズムは、本発明に係る重要な特徴である。特に、個々の鍵データ２２を、設定期間内において設定回数以上は使用しないという使用回数制限の採用は、鍵データサイズを実用的な範囲内に収めるために重要である。

【００２８】

以下には、このようなセキュリティ方式を採用した認証タグ生成アルゴリズムの作用効果を明示する観点から、図４に示すような具体的な鍵データテーブルを使用した認証タグ生成処理について順次説明する。

【００２９】

図４に示す鍵データテーブルは、送信目的の本体データとなる最大数「ｓ」個の送信目的データ「No.１」～「No.ｓ」に対して、ｋ個の鍵データ「No.１」～「No.ｋ」を用意した場合を示している。ここで、この鍵データテーブル中の鍵データの使用回数制限が、例えば、保護制御計測装置を運用開始してから、設定期間「２０年間」の間に設定回数「２回」以上は使用しない、という内容であるものとする。言い換えれば、使用回数制限は、「鍵データの繰り返し使用禁止回数の下限の設定回数が２回で、かつ、鍵データの繰り返し使用回数の上限が１回」、という内容であるものとする。

【００３０】

この使用回数制限を確実に守るためには、用意する鍵データの設定数ｋを事前に求めておく必要がある。ここで、用意する鍵データの設定数ｋは、運用期間の設定期間中に送信する「送信目的の本体データの総数」、すなわち、「送信目的の本体データの送信回数合計」に応じて容易に決定することができる。例えば、保護リレー装置の端子間データ授受において、相手端子に自端子の電流情報を６００Ｈｚ（５０Ｈｚ系統で電気角３０度）でサンプリングして６００Ｈｚで送る場合、設定期間「２０年間」中における送信目的の本体データの送信回数合計は、次の式（１）で求められる。

$$600\times60\times60\times24\times365\times20=3.8\times10^{11} \quad \cdots \quad (1)$$

【００３１】

この場合、用意する鍵データの数ｋを、この送信回数合計より大きく設定することにより、上記の使用回数制限「鍵データの繰り返し使用禁止回数の下限の設定回数が２回で、かつ、鍵データの繰り返し使用回数の上限が１回」を確実に守りながら、図４に示す鍵データテーブル中の鍵データを順次用いて認証タグを生成することができる。

【００３２】

具体的には、保護制御計測装置の運用開始時点で、例えば、最小番号の鍵データ「No.１」を初回として、鍵データを昇順に順次用いて認証タグを生成し、生成した認証タグを送信目的データに付加して、図３に示したフォーマットで相手装置へ順次送出していく。

【００３３】

ここで、図４に示す送信目的データの最大数「ｓ」は、送信目的データの取りうる総数

であり、例えば、送信目的データが３２ビット長の場合、ｓは2^{32}となる。また、認証タグが取りうる総数をｍとすれば、認証タグは$2^{\log m}$ビットで表現される。例えば、ある送信目的データNo.ｙを送信する際、使用する鍵データがNo.ｘであるとすると、送信目的データNo.ｙには、認証タグとして鍵データテーブルの認証行列の要素A_{xy}を付加する。

【００３４】

以上の場合に、認証タグ生成手段１３においては、最大でｍ種類の認証タグが生成される可能性があり、そのためには、設定期間「２０年間」の間に、サンプリング毎に異なる鍵データ「No.１」～「No.ｋ」を順番に使うことになる。

【００３５】

このように最大でｍ種類の認証タグを生成する認証タグ生成アルゴリズムを採用した場合に、悪意のある第３者（以下には、アタッカー(opponent)と称する）が、全くこのデータを盗み見ることなしに偽造データを作成して送った場合、あるいは、このデータを伝送路の途中で盗み読みして、これを元に偽造データを作成して送った場合を想定する。この場合に、受信側装置がその偽造データを正しいデータとして誤認してしまう確率は、１／ｍとなることが非特許文献２にて証明されている。

【００３６】

したがって、ＩＴ産業で一般的に用いられている計算量的な認証方式とは異なり、毎回のデータ伝送毎に異なる鍵を使用して最大でｍ種類の認証タグを生成する本実施形態の認証タグ生成アルゴリズムによれば、アタッカーにとってはその鍵を特定し、認証タグを偽造し、それが偶然正しい認証タグと合致する確率は１／ｍである。

【００３７】

計算量的な認証方式ではアタッカーにより高速なコンピュータによって一度鍵が判明すると、その後は完全になりすましあるいは改ざんが行われてしまうが、本実施形態の認証タグ生成アルゴリズムによれば、偽造された認証タグが正しい認証タグと合致する確率は２０年間で１／ｍであるため、このｍを大きく設定することによりアタッカーからの攻撃を実用上問題ないレベルで防御できる。

【００３８】

例えば、ｍ＝2^{32}であれば、アタッカーが認証タグの偽造に成功する確率は約10^{-9}となり、これは、保護制御計測装置に一般的に用いられているマイクロ波、光ファイバなどの伝送路の誤り率の範囲である10^{-5}～10^{-7}に比べて十分に小さく、無視できる範囲といえる。

【００３９】

図５は、認証タグ生成手段１３による認証タグ生成処理を示すフローチャートである。この図５に示すように、初回は鍵データ番号ｘをｘ＝１として（Ｓ５０１）、新規の送信目的データｙが発生する毎（Ｓ５０２）に、番号ｘの鍵データ「No.ｘ」を選択し、鍵データテーブルの認証行列の要素A_{xy}を認証タグとして、送信目的データｙに付加して送信する（Ｓ５０３）。

【００４０】

このように送信目的データを送信する毎に、使用する鍵データ番号ｘを１ずつ増分して次の鍵データ「No.ｘ＋１」に移行する（Ｓ５０４）。そして、新規の送信目的データを送信する毎に鍵データ番号ｘを１ずつ増分する一連の処理（Ｓ５０２～Ｓ５０４）を繰り返した後、最終的に最大の鍵データ番号「No.ｋ」まで達した時点（Ｓ５０５のＹＥＳ）で、再び鍵データ番号ｘをｘ＝１に戻して（Ｓ５０１）、一連の処理（Ｓ５０２～Ｓ５０４）を継続する。

【００４１】

このような認証タグ生成処理を行う場合に、予め準備しておく具体的な鍵データの数は、「設定期間中における送信目的の本体データの送信回数合計」を、使用回数制限による「鍵データの繰り返し使用回数の上限」で割り算することによって、容易に決定することができる。すなわち、「鍵データの繰り返し使用回数の上限が１回」である場合には、「設定期間中における送信目的の本体データの送信回数合計」を、「１」で割ることになる

ため、具体的な鍵データの数は、「送信回数合計」と同数以上であればよい。また、「鍵データの繰り返し使用回数の上限が２回」である場合には、「設定期間中における送信目的の本体データの送信回数合計」を、「２」で割ることになるため、具体的な鍵データの数は、「送信回数合計」の１／２倍以上であればよい。

【００４２】

［効果］

以上のような第１の実施形態によれば、次のような効果が得られる。まず、送信目的の本体データと、この本体データから生成された認証タグとを組み合わせてなるデータを送信し、受信側では受信したデータ中の本体データを元に生成した認証タグと、受信データ中に含まれている認証タグとを比較することで、伝送路上でのデータ改ざんの有無を検出できる。認証タグを生成する際に使用する鍵データは、データを送信する度に変更することで、計算量的観点ではなく情報量的観点からセキュリティを保証できる。

【００４３】

また、同じ鍵データを、設定期間内に設定回数以上使用しないという使用回数制限を採用したことで、保護制御計測装置の寿命から勘案した運用期間を設定期間とし、設定回数を少なくすることにより、運用期間中における改ざん、なりすましの発生確率を極めて小さくできる。特に、設定期間という時間的制限を設けたことで、鍵データサイズを無限に大きくすることなく、保護制御装置の運用上で実現可能な程度の範囲内に鍵データサイズを収めることが可能となる。

【００４４】

したがって、第１の実施形態によれば、鍵データサイズが実用上実現できる範囲内に収まり、かつ、保護制御計測用として実装が容易な実用的な情報量的セキュリティ技術を構築し、そのような情報量的セキュリティ技術を使用した安全性・信頼性の高い保護制御計測システムと装置、およびデータ伝送方法を提供することができる。

【００４５】

［第２～第７の実施形態］

以下に説明する第２～第７の実施形態に係る保護制御計測システムは、いずれも、第１の実施形態と同様のシステム構成を有する保護制御計測システム（図１）であり、第２～第５の実施形態は、処理・データ構成を部分的に変更、または、手段を追加した変形例であり、第６、第７の実施形態は、電流差動保護システムおよび変電所制御システムへの適用例である。そのため、第２～第７の実施形態の説明においては、第１の実施形態と異なる特徴のみを記載し、第１の実施形態と同一部分については、基本的に説明を省略するものとする。

【００４６】

［第２の実施形態］

前述した第１の実施形態では、鍵データとして、図４に示すような鍵データテーブル、認証行列を使用したが、第２の実施形態は、さらに、鍵データを、共通に使用する固定鍵行列Ｕと、送信毎に変更する使い捨て鍵ベクトルｖに分離する特徴を有することにより、認証タグおよび鍵データのサイズを小さくして、認証タグ生成演算量も小さくするものである。

【００４７】

そして、鍵データを固定鍵行列Ｕと使い捨て鍵ベクトルｖに分離した結果、認証タグ生成手段１３（図１）による認証タグ生成アルゴリズムは、認証タグベクトルｙを以下のベクトル演算で求めるという特徴を有する。

$$y = xU + v$$

ここで

ｘ：本体データベクトル

Ｕ：固定鍵行列

ｖ：使い捨て鍵ベクトル

【００４８】

図６は、このような認証タグ生成アルゴリズムを用いた第２の実施形態において、送信側装置１Ｔと受信側装置１Ｒにおける特徴的な認証タグ生成アルゴリズムと認証アルゴリズムを示す図である。

【００４９】

この図６に示すように、送信側装置１Ｔにおいては、上記のような認証タグ生成アルゴリズム６１により固定鍵行列Ｕと使い捨て鍵ベクトルｖを用いて本体データベクトルｘから認証タグベクトルｙが生成され、送信データ（ｘ，ｙ）として送信される。

【００５０】

また、受信側装置１Ｒにおいては、受信データ（ｘ’，ｙ’）を受信した場合に、認証アルゴリズム６２により、自装置内の固定鍵行列Ｕと使い捨て鍵ベクトルｖを用いて受信データ（ｘ’，ｙ’）中の本体データベクトルｘ’から認証タグベクトルｙ”が生成され、受信データ（ｘ’，ｙ’）中の認証タグベクトルｙ’との比較により認証判定が行われる。

【００５１】

このような第２の実施形態においては、鍵データを固定鍵行列Ｕと使い捨て鍵ベクトルｖに分離したことにより、使い捨て鍵ベクトルｖを操作するのみで、第１の実施形態により実現される認証タグ空間と同程度の大きな認証タグ空間を生成可能であるため、アタッカーに対して第１の実施形態と同程度の安全性・信頼性を確保できる。また、データ送信毎に変化させなければならない鍵データは、使い捨て鍵ベクトルｖのみであり、換言すれば、１つの固定鍵行列Ｕと送信回数に応じた必要数の使い捨て鍵ベクトルｖにより、鍵データを構成できるため、予め保護制御計測装置１に記憶すべき鍵データ量を小さくできる。

【００５２】

図７は、本実施形態による認証タグ生成アルゴリズムによるベクトル演算の具体例を示している。この図７の例においては、予め固定鍵行列Ｕが固定的に与えられており、ある本体データｘ（１，０，０，１，０）を送信するタイミングで、使い捨て鍵ベクトルｖが（０，１，０）であった場合、図中のように認証タグベクトルｙ（１，１，０）が生成される。受信側でも、受信データに対して同様の演算を実行して認証タグベクトルを算出し、受信データに付加されている認証タグベクトルと比較する。

【００５３】

以上のような第２の実施形態によれば、第１の実施形態と同等の効果が得られることに加えて、さらに、認証タグおよび鍵データのサイズを小さくして、認証タグ生成演算量も小さくすることができる。特に、本実施形態による認証タグ生成アルゴリズムは、ビット列の論理和と論理積をとるのみで認証タグベクトルを求められることから、高速演算可能であるため、保護制御計測装置のようなリアルタイム系、組み込み系の実装に適している。

【００５４】

また、設定期間「２０年間」で必要とする鍵データ全体のサイズは、以下の計算で求められ、約１．５テラバイトとなる。この値は、２００８年時点で保護制御計測装置に組み込むには大きい値であったが、記憶容量の増大化が急激に進んでいるメモリー製品の著しい開発現状からすれば、容易に実装可能な値となりつつある。

【００５５】

送信レート：600Hz
送信データ長：2047ビット
運用期間：20年
認証タグのビット数：32ビット（改ざん成功確率１／2^{32} = 10^{-9}）
必要な鍵サイズ＝(Uのサイズ＋vのサイズ)
= 32bit×2047bit + 32×(20年間の送信回数)
= 32×(2047 + 600×60×60×24×365×20)

$= 4\text{Bytes} \times 3.8 \times 10^{11}$
$= 1.5\text{T Bytes}$

【００５６】
［第３の実施形態］
前述した第１の実施形態では、受信側装置１Ｒにおいて、受信データ認証手段１５による認証の判定結果２５を出力する場合について説明したが、実際の受信側装置１Ｒでは、概して、受信データ２４ａ中の本体データ２１ａを用いて保護制御演算を行うアプリケーションを有する。

【００５７】
第３の実施形態は、このようなアプリケーションにおける不正データの使用を防止するために受信側装置におけるデータ処理に特徴を有するものであり、図８は、そのような受信側装置１Ｒにおける特徴的なデータ処理とデータの流れを示す図である。

【００５８】
図８に示すように、第３の実施形態は、アプリケーション８１に対して、受信データ２４ａ中の本体データ２１ａだけでなく、受信データ認証手段１５の判定結果２５を与えることにより、受信データ２４ａが不正なデータである場合に、その受信データ２４ａをアプリケーション８１で破棄するようにしたものである。また、判定結果２５をセキュリティ情報ログ手段８２に保存するようにしたものである。

【００５９】
図９は、このように受信データ認証手段１５の判定結果２５の取扱いに特徴を有する第３の実施形態において、受信側装置１Ｒにおける送受信手段１４と受信データ認証手段１５による特徴的なデータ処理を示すフローチャートである。

【００６０】
すなわち、受信側装置１Ｒで送受信手段１４によりデータを受信した場合（Ｓ９０１）に、受信データ認証手段１５は、受信データ２４ａの認証処理を実行して（Ｓ９０２）、判定結果２５をセキュリティ情報ログとしてセキュリティ情報ログ手段８２に保存する（Ｓ９０３）。アプリケーション８１に対して、送受信手段１４から本体データ２１ａを渡すと共に、受信データ認証手段１５から判定結果２５を渡す（Ｓ９０４）。

【００６１】
なお、図８中では、送受信手段１４からアプリケーション８１に本体データ２１ａを渡すデータの流れが記載されているが、受信データ認証手段１５により判定結果２５と本体データ２１ａの両方を渡してもよい。いずれにしても、アプリケーション８１に本体データ２１ａと判定結果２５の両方を渡すことにより、アプリケーション８１は不正な受信データ中の本体データを破棄することができる。

【００６２】
以上のような第３の実施形態によれば、第１の実施形態と同等の効果が得られることに加えて、さらに、不正なデータを保護制御演算に使用することを防止できるため、保護制御計測装置の信頼性を向上できる。また、不正データ受信時の判定結果をセキュリティ情報ログとして保存することで、保存したログを利用してアタッカーの攻撃様相を分析することが可能となるため、例えば、認証タグ生成アルゴリズムをさらに強固にするために認証タグのサイズを大きくする対策、あるいは、伝送路の監視などの各種の有効な対策を実施することが可能となる。

【００６３】
［第４の実施形態］
第４の実施形態は、送信側装置１Ｔと受信側装置１Ｒとの間で使用する鍵データを一致させるために、鍵データ保存手段１２（図１）に保存する鍵データ情報に、個々の鍵データを一意に特定する鍵識別情報を追加したものである。

【００６４】
図１０は、このような第４の実施形態の特徴的なデータ処理とデータの流れを示す図であり、送信側装置１Ｔと受信側装置１Ｒは、同じ鍵データ情報テーブル１０１を保持して

おり、鍵データ情報テーブル１０１には、複数の鍵データと、個々の鍵データを一意に特定する鍵識別情報が含まれる。図１０の例では、ｎ個の鍵データＫ１～Ｋｎに対して、鍵識別情報の一例として、シーケンス番号「１，２，…，ｎ」がそれぞれ付加されている。このような鍵データ情報テーブル１０１を使用した場合には、送信側装置１Ｔと受信側装置１Ｒでは、鍵を特定するシーケンス番号ｘを含むデータが生成されることになる。

【００６５】

すなわち、送信側装置１Ｔにおいて、認証タグ生成手段１３は、本体データ２１とシーケンス番号ｘの鍵データ２２から認証タグ２３を生成した場合に、本体データ２１から生成された認証タグ２３と、使用した鍵データ２２を特定するシーケンス番号ｘからなるデータセット１０２を送受信手段１４に渡す。その結果、送受信手段１４で生成される送信データ２４には、本体データ２１と認証タグ２３、および、鍵のシーケンス番号ｘが含まれる。

【００６６】

また、受信側装置１Ｒにおいて、送受信手段１４は、受信データ２４ａを、本体データ２１ａと鍵のシーケンス番号ｘからなるデータセット１０３と認証タグ２３ａに分離して、データセット１０３を認証タグ生成手段１３に渡す。認証タグ生成手段１３は与えられたシーケンス番号ｘに基づいて、自装置内の鍵データ情報テーブル１０１から同じシーケンス番号ｘの鍵データ２２を特定し、このシーケンス番号ｘの鍵データ２２と受信データ仲の本体データ２１ａを使用して比較対照用の認証タグ２３ｂを生成する。

【００６７】

これにより、送信側装置１Ｔと受信側装置１Ｒとの間で、同じ鍵データを使った認証処理が実現できる。

【００６８】

前述したように、第１の実施形態の認証方式においては、設定期間に同じ鍵データを使う回数を制限する使用回数制限を採用しているため、短い時間で区切って観測すれば、常に異なる鍵データを使用して認証タグを生成していることとなる。したがって、常に送受信側で使用する鍵データを一致させる仕組みが必要である。

【００６９】

これに対して、以上のような第４の実施形態によれば、鍵データを特定するシーケンス番号を使用することにより、送信側と受信側で使用する鍵データを確実に一致させることができる。例えば、万一、いずれかの保護制御計測装置が故障となり、一時的に伝送路が途絶えた後に復旧して送信を再開したとしても、本実施形態によれば、受信側でシーケンス番号を鍵データ情報テーブル１０１から探すことで、送信側と同じ鍵データを受信側で容易かつ確実に使用することができる。また、保護制御計測装置の運用を両端子で始める際にも、本実施形態によれば自動的に両端子で使用する鍵データの同期がとれることになるため、信頼性、運用性の高い保護制御計測システムを提供できる。

【００７０】

［第５の実施形態］

前述したように、第１または第２の実施形態の認証方式によれば、使用する鍵データの内容あるいはそれを使用する認証タグ生成アルゴリズムに応じて、不当な受信データを誤って正当と判定してしまう確率を明示的に決めることができる。

【００７１】

したがって、第５の実施形態としては、例えば、図１中の認証タグ生成手段１３に、使用する鍵データの内容および認証タグ生成アルゴリズムを利用者によって設定できる機能を設ける。このような構成とすることにより、正当でない受信データを誤って正当と判断してしまう確率を、例えば、伝送路の誤り確率以下になるように設定することが容易に可能となる。

【００７２】

従来提案されている保護制御計測システム用のセキュリティシステムは、ＩＴ産業で提案されているものが多く、保護制御技術者が、そのアルゴリズムや検出確率を制御するこ

とはできなかった。しかし、認証タグ生成手段１３に設定機能を設けた第５の実施形態によれば、アルゴリズムおよびこれから一意に決定される改ざん、なりすましの検出確率は、保護制御技術者でも容易に制御できることになる。

【００７３】
この場合の具体的な設定値としては、リレーの整定操作と同様に、例えば、
Ｕ，Ｖ，確率Ｐ，…
などのパラメータを順次整定していけばよい。例えば、伝送路の誤り率が10^{-5}であれば、10^{-6}以上となるように各種パラメータを定めて入力していけば、アタッカーによる攻撃を実用上はほとんど無視できる程度に防止可能となる。

【００７４】
技術開発に伴い、保護制御計測用の通信インフラが将来的に変わっていったとしても、本実施形態によれば、情報理論的に安全な保護制御計測システムを通信インフラの変化に影響されずに運用でき、コンピュータの処理能力の増大に脅かされることもなく、装置納入後のセキュリティソフトウェアの変更も不要となる。したがって、経済性、信頼性、稼働率の高い保護制御計測システムを提供できる。

【００７５】
［第６の実施形態］
図１１は、本発明を適用した第６の実施形態に係る保護制御計測システムを示しており、特に、第１の実施形態の保護制御計測システムを電流差動保護システムに適用した場合の特徴的なデータ処理とデータの流れを示す図である。

【００７６】
この図１１に示すように、電流差動保護システムは、送電線１１０の両端に保護リレー装置１１１，１１２を設置し、これらの保護リレー装置１１１，１１２間で自端の電流／電圧データ１１３を送信目的データとして互いに送信することで、キルヒホッフの法則に基づいた送電線の保護を実施するシステムである。

【００７７】
送電線の保護を実施するために、保護リレー装置１１１，１１２は、電流差動演算手段１１４を備えており、この電流差動演算手段１１４によって、自端の電流／電圧データ１１３と相手端の電流／電圧データ１１３ａを用いた電流差動演算を行い、事故検出時には、電流差動演算手段１１４からトリップ指令１１５を出力して自端の遮断器１１６をトリップする。以下には、このような電流差動保護システムにおいて、一方の保護リレー装置１１１の電流／電圧データ１１３を他方の保護リレー装置１１２で受信して電流差動演算を行う場合の処理について説明する。

【００７８】
保護リレー装置１１１は、目的データ取得手段１１（図１）によって送電線１１０の自端の電流／電圧データ１１３を取り込む。そして、電流／電圧データ１１３と鍵データ２２を認証タグ生成手段１３に入力し、認証タグ２３を生成する。この認証タグ２３と電流／電圧データ１１３を送受信手段１４に与え、送受信手段１４によって、電流／電圧データ１１３と認証タグ２３を組み合わせてなる送信データ２４を相手端の保護リレー装置１１２に送信する。

【００７９】
保護リレー装置１１２は、相手端の保護リレー装置１１１からのデータを受信データ２４ａとして送受信手段１４で受信すると、その受信データ２４ａ中に含まれる、相手端の保護リレー装置１１１の電流／電圧データ１１３ａを電流差動演算手段１１４に渡す。同時に、その同じ電流／電圧データ１１３ａと鍵データ２２を認証タグ生成手段１３に入力して、比較対照用の認証タグ２３ｂを生成する。

【００８０】
生成した比較対照用の認証タグ２３ｂと、受信データ２４ａ中の認証タグ２３ａを受信

データ認証手段１５に入力し、受信データ認証手段１５によって、これら２つの認証タグ２３ａ，２３ｂが一致するか否かの認証判定を行い、その判定結果２５を電流差動演算手段１１４に渡す。電流差動演算手段１１４には、目的データ取得手段１１（図１）によって取り込まれた自端の電流／電圧データ１１３も渡される。

【００８１】

電流差動演算手段１１４は、自端の電流／電圧データ１１３と、相手端の電流／電圧データ１１３ａを使って電流差動演算を実行し、送電線１１０の系統事故を検出した場合には、自端の遮断器１１６にトリップ指令１１５を出力する。

【００８２】

電流差動リレーシステムの場合、同時に逆方向の処理（保護リレー装置１１２が自端の電流／電圧データ１１３を保護リレー装置１１１に送信し、保護リレー装置１１１にて電流差動演算を実行し、系統事故を検出した場合は保護リレー装置１１１の自端の遮断器１１６をトリップする処理）も実行する。

【００８３】

図１２は、実際の電流差動リレーシステムに適用した場合のより具体的なイメージを示す。リレーが双方に自端の電気量データを送りあうことで保護システムを実現している。図中に吹き出しで示すフォーマット１２０は、イーサネット（登録商標）などの汎用の通信ネットワークの場合、１つの送信データ単位（フレーム）は、ヘッダ、電気量データ、認証タグ、およびＣＲＣ(Cyclic Redundancy Check)から構成されることを表す。イーサネットの場合、１フレームあたりの最大長は１５１４バイトであるので、認証タグのサイズが３２ビットの場合には、この認証タグの大きさ３２ビット（攻撃成功確率が10^{-9}）が、フレーム全体に占める割合はごくわずかであり、認証タグを付加することで通信量に与える影響は殆どないことがわかる。

【００８４】

以上のような第６の実施形態によれば、送電線電流差動保護リレーのように、保護制御用データを伝送路を介して互いに送受信する保護リレーに対して有効なセキュリティ対策が可能となる。

【００８５】

［第６の実施形態の変形例］

図１３は、図１１に示す第６の実施形態の電流差動保護システムにおいて、判定結果２５が「認証タグ不一致」（不正なデータ）である場合に、相手端の電流／電圧データを零として電流差動演算を実施する処理を示すフローチャートである。判定結果２５が「認証タグ一致」（正当なデータ）である場合にのみ、受信した相手端の電流／電圧データを使って電流差動演算を実施する。このような処理を行うことにより、不正なデータを電流差動演算に使用することを防止できるため、より信頼性の高い電流差動保護システムを提供できる。

【００８６】

図１４は、図１１に示す第６の実施形態の電流差動保護システムにおいて、判定結果２５が「認証タグ不一致」の場合に、電流差動演算の演算結果に関わらず、遮断器１１６へのトリップ指令をロックする処理を表す論理回路図である。

【００８７】

通常のリレーでは、電流差動演算の結果をそのままトリップ指令として遮断器１１６に出力するが、この図１４に示す例では、電流差動演算の結果と認証の判定結果２５とをアンド演算し、その結果を遮断器１１６に出力することで、判定結果２５が「認証タグ不一致」の場合にのみ、遮断器１１６にトリップ指令を出さないようにできる。このような処理を行うことにより、不正なデータに基づく遮断器のトリップを防止できるため、より信頼性の高い電流差動保護システムを提供できる。

【００８８】

［第７の実施形態］

図１５は、本発明を適用した第７の実施形態に係る保護制御計測システムを示しており、特に、第１の実施形態の保護制御計測システムを変電所制御システムに適用した場合の特徴的なデータ処理とデータの流れを示す図である。

【００８９】

この図１５に示すように、変電所制御システムは、変電所外部の制御用コンピュータ１５０１から、変電所内に設置された制御装置１５０２に対して制御指令１５０３を送信することにより、制御装置１５０２が管轄する電力用設備を制御するシステムである。

【００９０】

図１５では、一例として、制御用コンピュータ１５０１からの制御指令１５０３に応じて、制御装置１５０２の制御指令出力手段１５０４から制御信号１５０５を出力して変電所内の遮断器１１６を開閉制御するシステムを示している。また、制御用コンピュータ１５０１には、操作端末１５０６が接続されている。以下には、この操作端末１５０６から操作員が遮断器１１６の操作指令１５０３を発行した場合のシステムの動作について説明する。

【００９１】

制御用コンピュータ１５０１に接続された操作端末１５０６から操作員により遮断器１１６の制御指令１５０３が発行された場合、この制御指令１５０３は、制御用コンピュータ１５０１の送受信手段１４および認証タグ生成手段１３に入力される。認証タグ生成手段１３は、制御指令１５０３と鍵データ２２を使用して認証タグ２３を生成する。送受信手段１４は、制御指令１５０３と認証タグ２３を組み合わせてなる送信データ２４を制御装置１５０２に送信する。

【００９２】

制御装置１５０２は、制御用コンピュータ１５０１から送信されたデータを受信データ２４ａとして送受信手段１４で受信すると、その受信データ２４ａ中に含まれる制御用コンピュータ１５０１からの制御指令１５０３ａを制御指令出力手段１５０４と認証タグ生成手段１３に入力する。認証タグ生成手段１３は、受信した制御指令１５０３ａと鍵データ２２を用いて比較対照用の認証タグ２３ｂを生成する。生成した比較対照用の認証タグ２３ｂと、受信データ２４ａ中の認証タグ２３ａを受信データ認証手段１５に入力し、受信データ認証手段１５によって、これら２つの認証タグ２３ａ，２３ｂが一致するか否かの認証判定を行い、その判定結果２５を制御指令出力手段１５０４に渡す。

【００９３】

制御指令出力手段１５０４は、判定結果２５が「認証タグ一致」（正当な制御指令）の場合にのみ、受信した制御指令１５０３ａに沿った制御信号１５０５を遮断器１１６に対して出力する。

【００９４】

以上のような第７の実施形態によれば、伝送路の途中で制御指令が書き換えられた場合でも、その不正な制御指令により誤って機器を制御することを防止できる。したがって、信頼性の高い変電所制御システムを提供できる。

【００９５】

［他の実施形態］

なお、本発明は、前述した実施形態に限定されるものではなく、本発明の範囲内で他にも多種多様な変形例が実施可能である。すなわち、図面に示した装置構成は本発明の実現に必要な最小限の機能構成を示す一例にすぎず、各手段の具体的なハードウェア構成およびソフトウェア構成は適宜選択可能である。例えば、本発明は、保護制御計測装置の送受信手段として、物理的に分離した送信部と受信部を設ける構成や、送信用と認証用の認証タグ生成手段を個別に設ける構成なども包含する。

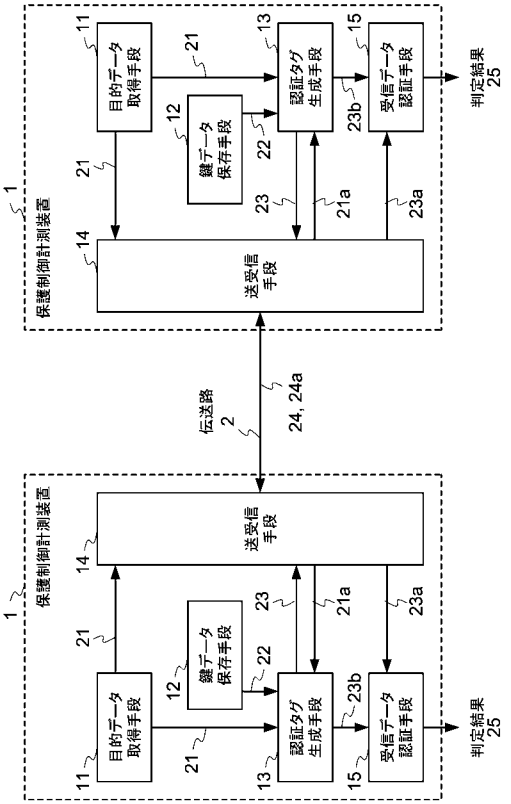
【図面の簡単な説明】

【００９６】

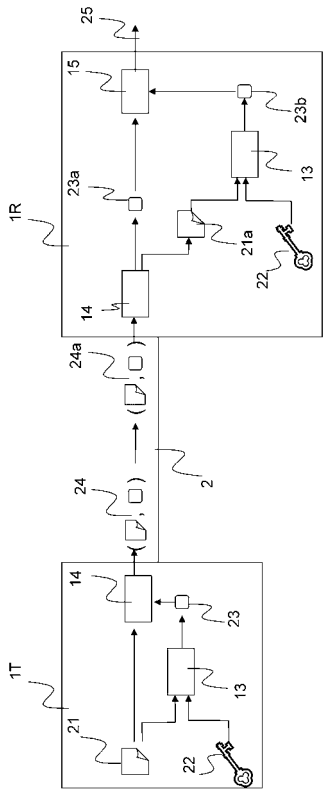
【図１】本発明を適用した第１の実施形態に係る保護制御計測システムの構成を示すブロ

ック図。
【図２】図１に示す保護制御計測システムにおける特徴的なデータ処理とデータの流れを示す図。
【図３】図１に示す保護制御計測装置間で送信される送信データのフォーマットを示す図。
【図４】図１に示す保護制御計測システムで使用する具体的な鍵データテーブルを示す図。
【図５】図１に示す認証タグ生成手段による認証タグ生成処理を示すフローチャート。
【図６】本発明を適用した第２の実施形態に係る保護制御計測システムにおける特徴的な認証タグ生成アルゴリズムと認証アルゴリズムを示す図。
【図７】図６に示す認証タグ生成アルゴリズムによるベクトル演算の具体例を示す図。
【図８】本発明を適用した第３の実施形態に係る保護制御計測システムの受信側装置における特徴的なデータ処理とデータの流れを示す図。
【図９】図８に示す受信側装置における送受信手段と受信データ認証手段による特徴的なデータ処理を示すフローチャート。
【図１０】本発明を適用した第４の実施形態に係る保護制御計測システムの特徴的なデータ処理とデータの流れを示す図。
【図１１】本発明を適用した第６の実施形態に係る電流差動保護システムの特徴的なデータ処理とデータの流れを示す図。
【図１２】図１１の電流差動保護システムのより具体的なイメージを示す図。
【図１３】図１１に示す第６の実施形態の変形例における特徴的なデータ処理を示すフローチャート。
【図１４】図１１に示す第６の実施形態の変形例における特徴的なデータ処理を示す論理回路図。
【図１５】本発明を適用した第７の実施形態に係る変電所制御システムの特徴的なデータ処理とデータの流れを示す図。
【符号の説明】
【００９７】
１…保護制御計測装置
３…伝送路
１１…目的データ取得手段
１２…鍵データ保存手段
１３…認証タグ生成手段
１４…送受信手段
１５…受信データ認証手段
２１…送信目的の本体データ
２１ａ…受信した本体データ
２２…鍵データ
２３…認証タグ
２３ａ…受信した認証タグ
２３ｂ…比較対照用の認証タグ
２４…送信データ
２４ａ…受信データ
２５…判定結果

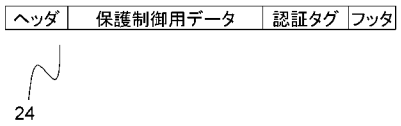
【図１】


保護制御計測装置
1
目的データ取得手段
11
鍵データ保存手段
12
認証タグ生成手段
13
受信データ認証手段
15
送受信手段
14
21
22
23
21a
23a
23b
判定結果
25
伝送路
2
24, 24a

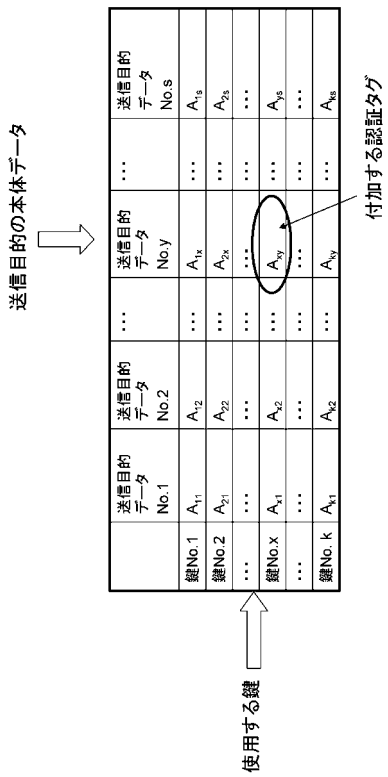
【図２】


1R
1T
2
14
15
13
21
22
23
21a
23a
23b
24
24a
25

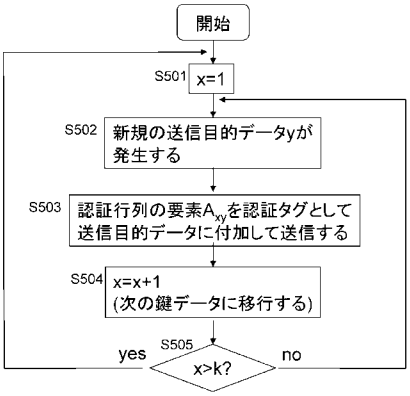
【図３】


ヘッダ
保護制御用データ
認証タグ
フッタ
24

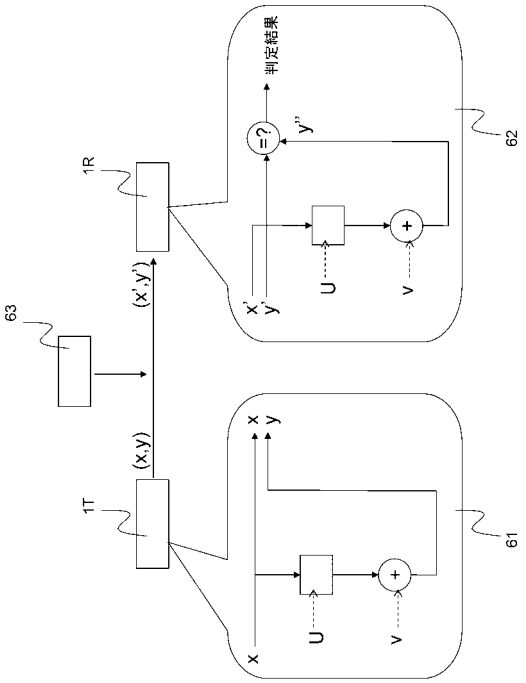
【図４】


送信目的の本体データ
付加する認証タグ
使用する鍵
送信目的データ No.1
送信目的データ No.2
送信目的データ No.y
送信目的データ No.s
鍵No.1
鍵No.2
鍵No.x
鍵No. k

【図５】



【図６】

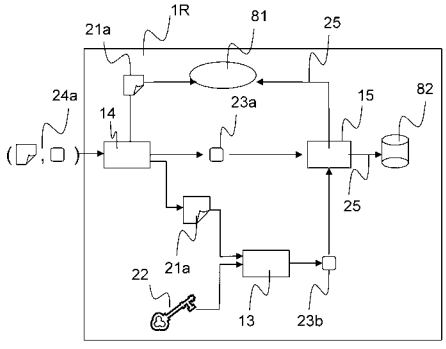


【図７】

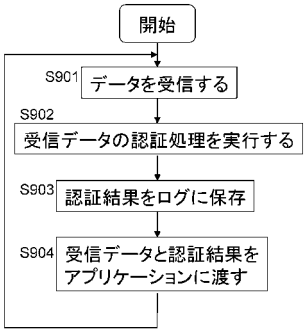
$$(1,1,0) = (1,0,0,1,0)\begin{pmatrix} 1&0&1 \\ 0&1&1 \\ 1&1&1 \\ 0&0&1 \\ 0&1&0 \end{pmatrix} + (0,1,0)$$

（y　x　U　v）

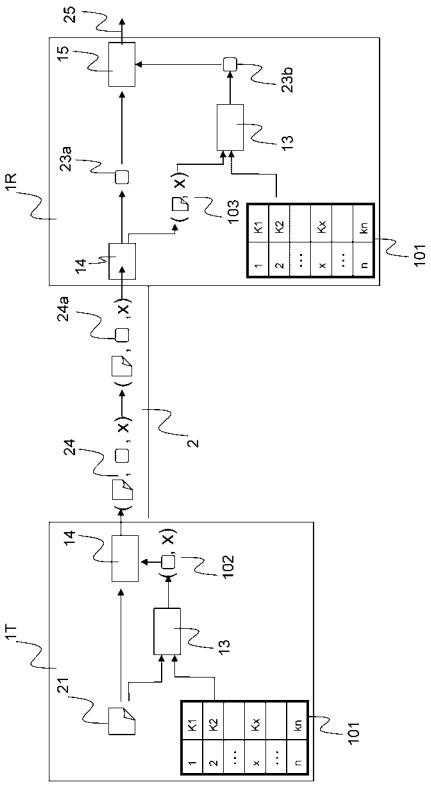
【図８】



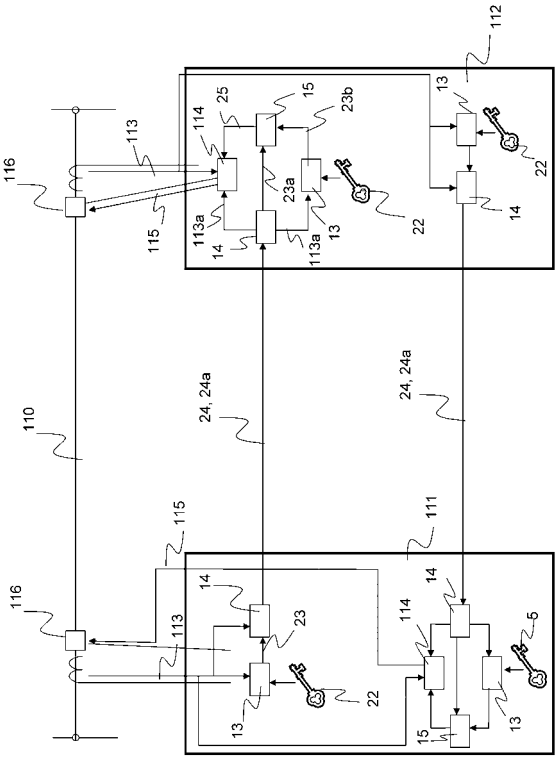
【図９】



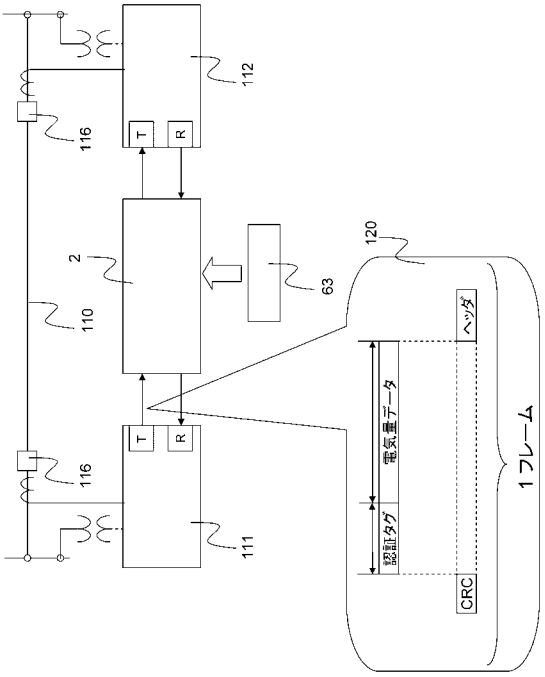
【図１０】



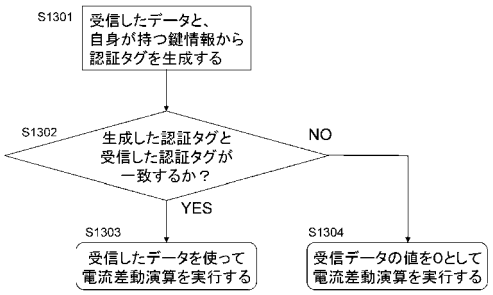
【図１１】



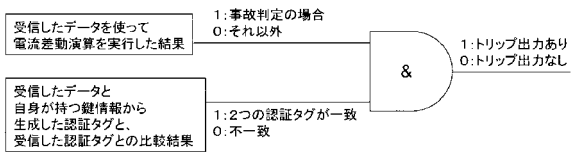
【図１２】



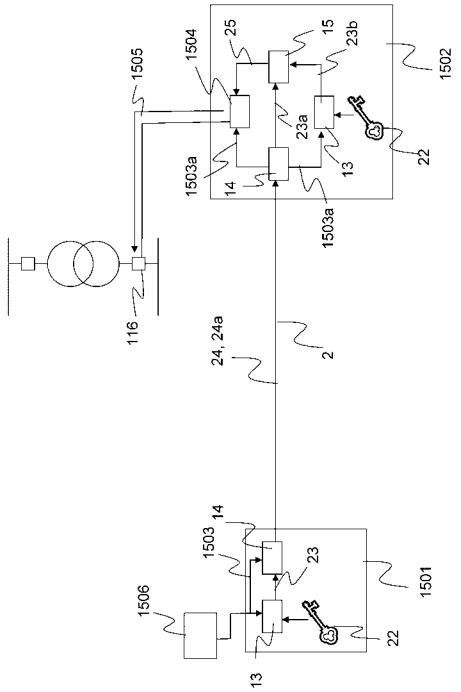
【図１３】



【図１４】



【図１５】


1505
1504
25
15
23b
1502
23a
22
1503a
14
13
1503a
116
24, 24a
2
14
1503
23
1501
1506
22
13

フロントページの続き

(72)発明者　福嶋　和人
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　松本　勉
神奈川県横浜市保土ケ谷区常盤台７９番１号　国立大学法人横浜国立大学内

審査官　青木　重徳

(56)参考文献　特開２００３－３３３０２３（ＪＰ，Ａ）
特開２００５－２１７９０７（ＪＰ，Ａ）
特開２００５－２０２４９７（ＪＰ，Ａ）
特開２０００－１９４２６２（ＪＰ，Ａ）
特開２０００－２９５２０９（ＪＰ，Ａ）
特開２０００－２２８８２１（ＪＰ，Ａ）
特開平１０－３０３８８１（ＪＰ，Ａ）
特開平１０－２６９１８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／１４