(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4222403号
(P4222403)
(45)発行日　平成21年2月12日(2009.2.12)　(24)登録日　平成20年11月28日(2008.11.28)

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

請求項の数 6　(全 23 頁)

(21)出願番号　特願2006-281908(P2006-281908)
(22)出願日　平成18年10月16日(2006.10.16)
(65)公開番号　特開2008-99214(P2008-99214A)
(43)公開日　平成20年4月24日(2008.4.24)
審査請求日　平成20年4月28日(2008.4.28)

（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　速水　雄太

最終頁に続く

(54)【発明の名称】不正端末推定システム、不正端末推定装置及び通信端末装置

(57)【特許請求の範囲】
【請求項１】
マルチホップネットワークにより複数の通信端末装置と不正端末推定装置が接続され、不正端末推定装置により不正な動作を行った通信端末装置を推定するシステムであって、
前記不正端末推定装置は、
ネットワークを形成する通信端末装置の識別情報や鍵情報を管理する通信端末情報管理部と、
前記不正な動作を推定するためのチャレンジ情報を生成する生成部と、
前記通信端末装置へ前記チャレンジ情報を送信する送信部と、
前記通信端末装置から前記チャレンジ情報に対応するレスポンス情報を受信する受信部と、
前記通信端末装置より返信された前記レスポンス情報に含まれる認証子が正しいか否かを検証するレスポンス情報検証部と、
検証の結果、前記レスポンス情報が正当なものでない場合に、上記各通信端末装置に受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置を推定する不正端末装置推定処理部と、を備え、
前記通信端末装置は、
他の通信端末装置もしくは前記不正端末装置から、直接又は配送中継により前記チャレンジ情報を受信する受信部と、
前記チャレンジ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、

他の通信端末装置から受信した前記レスポンス情報の返信経路上の通信端末装置及び自身における前記チャレンジ情報の受信を証明する認証子を生成する認証子生成部と、
他の通信端末装置から受信した前記レスポンス情報に自身が生成した前記受信証明情報及び前記認証子を加えて得られる前記受信生成情報を保持する受信生成情報格納部と、
前記受信証明情報及び前記認証子を含む前記レスポンス情報を生成するレスポンス情報生成部と、
他の通信端末装置又は前記不正端末装置へ、直接又は配送中継により前記レスポンス情報又は前記受信生成情報を送信する送信部と、
を備えることを特徴とする、不正端末推定システム。
【請求項２】
前記不正な動作を行った通信端末装置は、真正な通信端末装置に成りすました通信端末装置、又は真正なデータを改竄した通信端末装置であることを特徴とする、請求項１に記載の不正端末推定システム。
【請求項３】
マルチホップネットワークにより複数の通信端末装置と接続され、不正な動作を行った通信端末装置を推定する不正端末推定装置であって、
ネットワークを形成する通信端末装置の識別情報や鍵情報を管理する通信端末情報管理部と、
前記不正な動作を推定するためのチャレンジ情報を生成する生成部と、
前記通信端末装置へ前記チャレンジ情報を送信する送信部と、
前記通信端末装置から前記チャレンジ情報に対応するレスポンス情報を受信する受信部と、
前記通信端末装置より返信された前記レスポンス情報に含まれる認証子が正しいか否かを検証するレスポンス情報検証部と、
検証の結果、前記レスポンス情報が正当なものでない場合に、上記各通信端末装置に前記チャレンジ情報の受信を証明する情報を含む受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置を推定する不正端末装置推定処理部と、
を備えることを特徴とする、不正端末推定装置。
【請求項４】
前記チャレンジ情報を生成するチャレンジ情報生成部を更に備えることを特徴とする、請求項３に記載の不正端末推定装置。
【請求項５】
前記不正な動作を行った通信端末装置は、真正な通信端末装置に成りすました通信端末装置、又は真正なデータを改竄した通信端末装置であることを特徴とする、請求項３又は４に記載の不正端末推定装置。
【請求項６】
マルチホップネットワークにより複数の他の通信端末装置及び不正端末推定装置と接続される通信端末装置であって、
他の通信端末装置もしくは前記不正端末装置から、直接又は配送中継によりチャレンジ情報を受信する受信部と、
前記チャレンジ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、
他の通信端末装置から受信したレスポンス情報の返信経路上の通信端末装置及び自身における前記チャレンジ情報の受信を証明する認証子を生成する認証子生成部と、
他の通信端末装置から受信した前記レスポンス情報に自身が生成した前記受信証明情報及び前記認証子を加えた受信生成情報を保持する受信生成情報格納部と、
前記受信証明情報及び前記認証子を含む新たなレスポンス情報を生成するレスポンス情報生成部と、
他の通信端末装置又は前記不正端末装置へ、直接又は配送中継により前記新たなレスポンス情報又は前記受信生成情報を送信する送信部と、

を備えることを特徴とする、通信端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不正端末推定システム、不正端末推定装置及び通信端末装置に関する。
【背景技術】
【０００２】
近年、無線通信機能を持った多数のセンサ機器によって形成されるセンサネットワークが提案されている。ここで、センサネットワークは、通信端末間のパケットの送受信を、１つ以上の通信端末装置が中継配送するマルチホップネットワークであると想定する。
【０００３】
無線マルチホップネットワークにおいて、不正な中継端末装置の不正な振る舞いに対応できる技術として、例えば特許文献１には、ユーザからの要求に応じて基地局からユーザへ送信される情報に改竄や破壊等の不正行為が行われた時に、その地点を推定し、さらには不正地点を経由する経路が確立されないように経路確立を制御するアドホック無線ネットワークシステムおよびその不正管理方法が記載されている。
【０００４】
また、例えば特許文献２には、無線マルチホップネットワークにおいて不正パケットの投入を防止するために、ネットワークに認証済みの通信端末のみが知る第1の秘密情報を用いて第１のパケット検査データを作成するとともに、パケットの宛先端末との間で共有される第２の秘密情報を用いて第２のパケット検査データを作成し、作成した前記第１のパケット検査データ及び第２のパケット検査データを付加したパケットを生成することで、不正パケットの投入を防止する方法が記載されている。
【０００５】
【特許文献１】特開２００５－２８６９５６号公報
【特許文献２】特許第３７４９６７９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、センサネットワークを形成する無線通信端末装置は、一般的に低コストを重視して開発されるため、コスト高となる耐タンパ性メモリ（鍵情報などの秘密情報の漏洩・改竄を物理的に保護する装置）の搭載を必ずしも仮定できない。すなわち、ネットワークに認証済みの正当な通信端末装置が、攻撃者に鍵情報を不正に入手されることにより、不正に振る舞うという脅威が存在する。これら正当な（正当だと認識している）通信端末装置がマルチホップネットワークのパケット中継端末装置となることで、パケットの改竄等の不正な振る舞いを、認証された行為として実行できる。ネットワークを正常に機能させるためには、上記不正に振る舞う正当な（正当だと認識している）通信端末装置を検出する技術が必要になる。
【０００７】
上記従来の技術では、正当だと認識している通信端末装置による不正な振る舞いを想定していない。すなわち、パケットに付加されている検査データや署名の検証に成功しても、その検査データや署名が保証するパケットは必ずしも正当ではないことを想定していない。
【０００８】
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、中継途中でパケットの改竄や中継拒否等の妨害攻撃を行い、正当だと認識されている通信端末装置をネットワークから排除するために、不正を行った通信端末装置を推定することが可能な、新規かつ改良された不正端末推定システム、不正端末推定装置、及び通信端末装置を提供することにある。
【課題を解決するための手段】

【０００９】
上記課題を解決するために、本発明のある観点によれば、マルチホップネットワークにより複数の通信端末装置と不正端末推定装置が接続され、不正端末推定装置により不正な動作を行った通信端末装置を推定するシステムであって、前記不正端末推定装置は、ネットワークを形成する通信端末装置の識別情報や鍵情報を管理する通信端末情報管理部と、前記不正な動作を推定するためのチャレンジ情報を生成する生成部と、前記通信端末装置へ前記チャレンジ情報を送信する送信部と、前記通信端末装置から前記チャレンジ情報に対応するレスポンス情報を受信する受信部と、前記通信端末装置より返信された前記レスポンス情報に含まれる認証子が正しいか否かを検証するレスポンス情報検証部と、検証の結果、前記レスポンス情報が正当なものでない場合に、上記各通信端末装置に受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置を推定する不正端末装置推定処理部と、を備え、前記通信端末装置は、他の通信端末装置もしくは前記不正端末装置から、直接又は配送中継により前記チャレンジ情報を受信する受信部と、前記チャレンジ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、他の通信端末装置から受信した前記レスポンス情報の返信経路上の通信端末装置及び自身における前記チャレンジ情報の受信を証明する認証子を生成する認証子生成部と、他の通信端末装置から受信した前記レスポンス情報に自身が生成した前記受信証明情報及び前記認証子を加えて得られる前記受信生成情報を保持する受信生成情報格納部と、前記受信証明情報及び前記認証子を含む前記レスポンス情報を生成するレスポンス情報生成部と、他の通信端末装置又は前記不正端末装置へ、直接又は配送中継により前記レスポンス情報又は前記受信生成情報を送信する送信部と、を備える不正端末推定システムが提供される。

【００１０】
上記構成によれば、不正端末推定装置から通信端末装置へ不正な動作を推定するためのチャレンジ情報が送信され、通信端末装置から不正端末推定装置へチャレンジ情報に対応するレスポンス情報が送信される。レスポンス情報に含まれる認証子が正しいか否かが検証され、検証の結果、レスポンス情報が正当なものでない場合に、各通信端末装置に受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置が推定される。従って、マルチホップネットワークにより複数の通信端末装置が接続されたシステムにおいて、不正な動作を行った通信端末装置を推定することが可能となる。

【００１１】
また、前記不正な動作を行った通信端末装置は、真正な通信端末装置に成りすました通信端末装置、又は真正なデータを改竄した通信端末装置であっても良い。

【００１２】
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、マルチホップネットワークにより複数の通信端末装置と接続され、不正な動作を行った通信端末装置を推定する不正端末推定装置であって、ネットワークを形成する通信端末装置の識別情報や鍵情報を管理する通信端末情報管理部と、前記不正な動作を推定するためのチャレンジ情報を生成する生成部と、前記通信端末装置へ前記チャレンジ情報を送信する送信部と、前記通信端末装置から前記チャレンジ情報に対応するレスポンス情報を受信する受信部と、前記通信端末装置より返信された前記レスポンス情報に含まれる認証子が正しいか否かを検証するレスポンス情報検証部と、検証の結果、前記レスポンス情報が正当なものでない場合に、上記各通信端末装置に前記チャレンジ情報の受信を証明する情報を含む受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置を推定する不正端末装置推定処理部と、を備える不正端末推定装置が提供される。

【００１３】
上記構成によれば、通信端末装置へ不正な動作を推定するためのチャレンジ情報が送信され、チャレンジ情報に対応するレスポンス情報が通信端末装置から受信される。レスポンス情報に含まれる認証子が正しいか否かが検証され、検証の結果、前記レスポンス情報

が正当なものでない場合に、各通信端末装置に受信生成情報の配送を依頼し、配送された受信生成情報に基づいて、不正な動作を行った通信端末装置が推定される。従って、不正端末推定装置に接続された複数の通信端末装置のうち、不正な動作を行った通信端末装置を推定することが可能となる。

【００１４】

また、前記チャレンジ情報を生成するチャレンジ情報生成部を更に備えるものであっても良い。かかる構成によれば、不正端末推定装置で生成したチャレンジ情報を通信端末装置へ送ることができる。

【００１５】

また、前記不正な動作を行った通信端末装置は、真正な通信端末装置に成りすました通信端末装置、又は真正なデータを改竄した通信端末装置であっても良い。

【００１６】

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、マルチホップネットワークにより複数の他の通信端末装置及び不正端末推定装置と接続される通信端末装置であって、他の通信端末装置もしくは前記不正端末装置から、直接又は配送中継により不正な動作を推定するためのチャレンジ情報を受信する受信部と、前記チャレンジ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、他の通信端末装置から受信したレスポンス情報の返信経路上の通信端末装置及び自身における前記チャレンジ情報の受信を証明する認証子を生成する認証子生成部と、他の通信端末装置から受信した前記レスポンス情報に自身が生成した前記受信証明情報及び前記認証子を加えた受信生成情報を保持する受信生成情報格納部と、前記受信証明情報及び前記認証子を含む新たなレスポンス情報を生成するレスポンス情報生成部と、他の通信端末装置又は前記不正端末装置へ、直接又は配送中継により前記新たなレスポンス情報又は前記受信生成情報を送信する送信部と、を備える通信端末装置が提供される。

【００１７】

上記構成によれば、他の通信端末装置もしくは前記不正端末装置から、直接又は配送中継によりチャレンジ情報が受信され、チャレンジ情報の受信を証明する受信証明情報が生成され、他の通信端末装置から受信したレスポンス情報の返信経路上の通信端末装置及び自身における前記チャレンジ情報の受信を証明する認証子が生成され、他の通信端末装置から受信したレスポンス情報に自身が生成した受信証明情報及び認証子を加えた受信生成情報が保持される。そして、受信証明情報及び認証子を含む新たなレスポンス情報が生成される。不正端末推定装置での検証の結果、レスポンス情報が正当なものでない場合は、各通信端末装置から不正端末推定装置へ受信生成情報を配送することができ、配送された受信生成情報に基づいて、不正な振る舞いを行った通信端末装置を推定することができる。従って、不正に振る舞った通信端末装置を推定することが可能となる。

【発明の効果】

【００１８】

本発明によれば、不正な通信端末装置を確実に推定することが可能な、新規かつ改良された不正端末推定システム、不正端末推定装置、及び通信端末装置を提供することが可能となる。

【発明を実施するための最良の形態】

【００１９】

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。

【００２０】

以下に説明する実施形態では、マルチホップネットワークを形成する通信端末装置ＩＤｉが、受信したチャレンジ情報に対するレスポンス情報を生成し、生成したレスポンス情報を不正端末推定装置１００に配送し、不正端末推定装置１００が、上記レスポンス情報が正当か否かを検証し、検証が失敗することで、レスポンス情報の配送に関わった通信端

末装置ＩＤｉの中に不正に振る舞った通信端末装置ＩＤｉが存在することを判断し、不正端末推定装置１００が、上記各通信端末装置ＩＤｉに受信情報と生成情報の再送を依頼することによって、不正に振る舞った通信端末装置ＩＤｉを推定することを特徴とする。

【００２１】

本実施形態は、マルチホップネットワークを形成する複数の通信端末装置ＩＤｉの中で、不正に振る舞った通信端末装置ＩＤｉを推定する技術に関するものである。「不正に振る舞う」とは、例えば、マルチホップネットワークにおいて通信される情報を中継する通信端末装置ＩＤｉが、中継途中のメッセージを改竄したり、中継途中のメッセージを破棄（中継拒否）したりすることを想定する。

【００２２】

図１は、本発明の一実施形態における不正端末推定装置１００の内部構成を示すブロック図である。図１において、不正端末推定装置１００は、チャレンジ情報生成部１１０、通信端末情報管理部１２０、レスポンス情報検証部１３０、不正端末推定処理部１４０、受信生成情報検証部１５０、送信部１６０及び受信部１７０を有する。

【００２３】

チャレンジ情報生成部１１０は、チャレンジ情報を生成するものである。生成したチャレンジ情報を送信部１６０とレスポンス情報検証部１３０へ与える。チャレンジ情報は、例えば乱数情報であってもよいし、ネットワークを形成する各通信端末装置ＩＤｉに配送したいメッセージであっても良い。

【００２４】

通信端末情報管理部１２０は、ネットワークを形成する各通信端末が保持する識別情報、鍵情報を管理するものである。識別情報とは、ネットワークを形成する各通信端末に固有のビット列であり、例えば、各通信端末装置ＩＤｉに唯一のＭＡＣアドレスや、上記ネットワーク内でのみ唯一のネットワークアドレスなどを想定するが、特に限定するものではない。鍵情報とは、不正端末推定装置１００と各通信端末装置ＩＤｉとが１対１で秘密に共有する鍵情報を想定する。鍵情報は、鍵情報と供に再送攻撃を防止するためのカウンタ情報を保持していても良い。通信端末情報管理部１２０は、自身が管理する通信端末装置ＩＤｉの識別情報と鍵情報をレスポンス情報検証部１３０と受信生成情報検証部１５０へ与える。

【００２５】

レスポンス情報検証部１３０は、不正端末装置推定処理部１４０より与えられたレスポンス情報の認証子を、通信端末情報管理部１２０より与えられた鍵情報とチャレンジ情報生成部１１０より与えられたチャレンジ情報を用いて検証するものである。レスポンス情報検証部１３０は、検証結果が一致することにより、検証結果成功メッセージを、一方、検証結果が一致しないことにより、検証結果失敗メッセージを、不正端末装置推定処理部１４０へ返信する。

【００２６】

受信生成情報検証部１５０は、受信部１７０より与えられた受信生成情報に含まれる認証子（Ｇｉ）を、通信端末情報管理部１２０より与えられた、当該受信生成情報の送信元通信端末装置ＩＤｉの鍵情報を用いて検証し、検証に成功することで、当該受信生成情報と認証子（Ｇｉ）検証成功メッセージを不正端末装置推定処理部１４０へ与え、検証に失敗することで、認証子（Ｇｉ）検証失敗メッセージを不正端末装置推定処理部１４０へ与える。また、受信生成情報検証部１５０は、規定時間の間に、認証子（Ｇｉ）の検証に成功する受信生成情報を与えられなかったことを受けて、返信なしメッセージを不正端末装置推定処理部１４０へ与える。

【００２７】

送信部１６０は、チャレンジ情報生成部１１０より与えられたチャレンジ情報をネットワークの通信端末装置ＩＤｉに送信するものである。また、不正端末装置推定処理部１４０より与えられた、受信生成情報再送依頼メッセージを通信端末装置ＩＤｉへ送信するものである。

【００２８】
受信部１７０は、通信端末より受信したレスポンス情報を不正端末推定装置１００に与えるものである。また、通信端末より受信した受信生成情報を受信生成情報検証部１５０へ与えるものである。
【００２９】
通信端末装置ＩＤｉより不正端末推定装置１００へ返信されるレスポンス情報の一例を、図２に示す。図２に示すように、レスポンス情報には、レスポンス情報を配送中継した全ての通信端末装置ＩＤ１，ＩＤ２，ＩＤ３，…の識別子が含められる。図２において、認証子（Ｆ１，Ｇ１）とは、通信端末装置ＩＤ１と不正端末推定装置１００とが秘密に共有する鍵情報を利用して生成した情報である。不正端末装置よりｉホップ目の通信端末装置ＩＤｉの生成する受信生成情報を検証するための認証子Ｆｉは以下の式１で表される。
Ｆｉ＝Ｆ（ＫＩＤｉ，…，ＩＤｉ，Ｍ）　・・・（式１）
【００３０】
ここで、関数Ｆ（・）は、不正端末推定装置１００と通信端末装置ＩＤｉが秘密に共有する鍵（ＫＩＤｉ）と、レスポンス情報の配送中継に関わった通信端末装置ＩＤｉの識別子（…，ＩＤｉ）とチャレンジ情報（Ｍ）を入力とする値であり、例えば、レスポンス情報の配送中継に関わった通信端末装置ＩＤｉの前識別子とチャレンジ情報から構成されるビット列“…||ＩＤｉ||Ｍ”（||はビット連結を示す）に対して鍵情報ＫＩＤｉを利用して生成した、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）やＨＭＡＣ（Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を想定する。不正端末装置よりｉホップ目の通信端末装置ＩＤｉの生成する通信端末装置のチャレンジ情報の受信を検証するための認証子Ｇｉは以下の式２で表される。
Ｇｉ＝Ｇ（ＫＩＤｉ，…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)，ＩＤｉ，Ｆｉ）　・・・（式２）
【００３１】
ここで、関数Ｇ（・）は、不正端末推定装置１００と通信端末装置ＩＤｉが秘密に共有する鍵（ＫＩＤｉ）と、レスポンス情報の通信端末装置ＩＤｉまでの配送中継に関わった通信端末装置の識別子（…）と（存在しない場合もある）、通信端末装置(ｉ＋１)（不正端末装置よりｉ＋１ホップ目の通信端末装置で、通信端末装置ｉが中継依頼を受けた装置）の識別子（ＩＤ(ｉ＋１)）と、通信端末装置(ｉ＋１)から受信した認証子（Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）と（存在しない場合もある）、通信端末装置ＩＤｉの識別子（ＩＤｉ）と通信端末装置ＩＤｉの生成した認証子（Ｆｉ）を入力とする値であり、例えば、上記鍵ＫＩＤｉ以外の情報から構成されるビット列“…||ＩＤ(ｉ＋１)||Ｆ(ｉ＋１)||Ｇ(ｉ＋１)||ＩＤｉ||Ｆｉ”（||はビット連結を示す）に対して鍵情報ＫＩＤｉを利用して生成した、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）やＨＭＡＣ（Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を想定する。
【００３２】
レスポンス情報検証部１３０は、不正端末装置推定処理部１４０より、レスポンス情報と認証子（Ｇｉ）の検証依頼を与えられることにより、チャレンジ情報生成部１１０より与えられるチャレンジ情報Ｍと、通信端末情報管理部１２０より与えられる該当通信端末装置ＩＤｉの鍵情報を用いて、認証子（Ｇｉ）が正しいか否かを検証し、検証した結果を不正端末装置推定処理部１４０へ返信する。また、レスポンス情報検証部１３０は、不正端末装置推定処理部１４０より、レスポンス情報と認証子（Ｆｉ）の検証依頼を与えられることにより、チャレンジ情報生成部１１０より与えられるチャレンジ情報Ｍと、通信端末情報管理部１２０より与えられる該当通信端末装置ＩＤｉの鍵情報を用いて、認証子（Ｆｉ）が正しいか否かを検証し、検証した結果を不正端末装置推定処理部１４０へ返信する。
【００３３】

不正端末推定処理部１４０は、ネットワークに存在する不正な振る舞いを行った通信端末装置ＩＤｉを推定するものである。不正端末推定処理部１４０は、受信部１７０より与えられたレスポンス情報に付加されている認証子（Ｇｉ）を検証するために、上記レスポンス情報と認証子（Ｇｉ）の検証依頼をレスポンス情報検証部１３０へ与える。そして、レスポンス情報検証部１３０より、検証結果成功メッセージを返信されることにより、上記レスポンス情報の配送に関わった通信端末装置ＩＤｉ（レスポンス情報に含まれる識別子が示す全ての通信端末装置ＩＤｉ）を正当な通信端末装置であるとする。そして、チャレンジ情報Mが上記の通信端末装置に正しく届けられたことを知る。

【００３４】

一方、検証結果失敗メッセージを返信されることにより、上記レスポンス情報の配送に関わった通信端末装置ＩＤｉ（レスポンス情報に含まれる識別子が示す全ての通信端末装置ＩＤｉ）には不正な通信端末装置が潜む可能性があると判断し、不正端末推定処理を行う。不正端末推定処理は、上記不正な通信端末装置が潜む可能性があると判断された経路に存在する通信端末装置ＩＤｉに対して、不正端末推定装置１００からのホップ数が少ない通信端末装置ＩＤｉから順番（不正端末推定装置１００にレスポンス情報を最後に中継配送した通信端末装置ＩＤ１→ＩＤ２→ＩＤ３→…）に行ってゆく。

【００３５】

以下、図４及び図５のフローチャートを参照しながら、不正端末推定処理の手順を説明する。先ず、レスポンス情報の送信元が本当に通信端末装置ＩＤ１かどうかを検証するために、レスポンス情報と認証子（Ｆ１）の検証依頼を、レスポンス情報検証部１３０へ与える（図４のステップＳ２）。そして、レスポンス情報検証部１３０より、検証失敗メッセージを返信されることにより、以下２つの不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ４）。

【００３６】

・レスポンス情報の送信元端末は通信端末装置ＩＤ１ではない（通信端末装置ＩＤ１へのなりすまし攻撃が行われた）。
・通信端末装置ＩＤ１は不正な振る舞いを行った。

【００３７】

一方、検証成功メッセージを返信されることにより、不正端末推定処理部１４０は、レスポンス情報の送信元端末を通信端末装置ＩＤ１であると認証する。また、通信端末ＩＤ１には確かにチャレンジ情報Mが到達していることを知る（ステップＳ３）。次に、不正端末装置推定部１４０は、通信端末装置ＩＤ１に受信生成情報の配送を依頼するために、受信生成情報再送依頼メッセージを生成し、送信部１６０へ与える（ステップＳ５）。そして、受信生成情報検証部１５０より、受信生成情報が与えられるのを待つ（ステップＳ６）。受信生成情報検証部１５０は、受信生成情報Ｇｉを受けて、Ｇｉを検証する（ステップＳ７）。

【００３８】

ここで、受信生成情報の一例を図３に示す。図３において、通信端末装置の識別子（…，ＩＤ３，ＩＤ２）と、認証子（Ｆ２，Ｇ２）は、通信端末装置ＩＤ２より受信するレスポンス情報である。通信端末装置ＩＤ１の識別子（ＩＤ１）と、認証子（Ｆ１，Ｇ１）は、レスポンス情報が通信端末装置ＩＤ１を中継することで新たに発生する情報である。不正端末装置推定処理部１４０は、受信生成情報検証部１５０より認証子（Ｇ１）検証失敗メッセージを与えられることにより、以下の不正の可能性があることを検知する（ステップＳ９）。

【００３９】

・通信端末装置ＩＤ１は不正な振る舞いを行った（通信端末装置ＩＤ１は不正に振る舞ったことを検知されるのを恐れ、認証子検証に成功しない受信生成情報を返信した疑いがある）。
・受信生成情報の送信元端末は通信端末装置ＩＤ１ではない（通信端末装置ＩＤ１へのなりすまし攻撃が行われた）。

【００４０】
そして、受信生成情報検証部１５０より返信なしメッセージを与えられることにより、以下の不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ８）。
・通信端末装置ＩＤ１は不正な振る舞いを行った（通信端末装置ＩＤ１は不正に振る舞ったことを検知されるのを恐れ、受信生成情報の再送依頼を破棄した疑いがある）。
【００４１】
一方、不正端末装置推定部１４０は、受信生成情報検証部１５０より受信生成情報と、認証子（Ｇ１）検証成功メッセージを与えられることで、受信生成情報の検証処理を行う（ステップＳ１０）。受信生成情報の検証処理では、不正端末推定装置１００は、通信端末装置ＩＤ１より既に受信済みのレスポンス情報に含まれる情報（…，ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１）が、受信生成情報に含まれる情報と一致しているか否かを検証する（ステップＳ１１）。検証に失敗することで、以下の不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ１３）。
【００４２】
・通信端末装置ＩＤ１は不正な振る舞いを行った（通信端末装置ＩＤ１はレスポンス情報を中継時に改竄した疑いがある）。
【００４３】
一方、検証に成功することで、受信生成情報に含まれる情報のうち、「通信端末装置ＩＤ２から受信したレスポンス情報」が間違っていることを知る（ステップＳ１２）。次に、レスポンス情報を次に中継配送した通信端末装置ＩＤ２に関しても不正端末推定処理を行ってゆく（図５のステップＳ１４）。まず、通信端末装置ＩＤ１の受信生成情報に含まれる「通信端末装置ＩＤ２から受信したレスポンス情報」の送信元が本当に通信端末装置ＩＤ２かどうかを検証するために、上記レスポンス情報と認証子（Ｆ２）の検証依頼を、レスポンス情報検証部１３０へ与える（ステップＳ１５）。そして、レスポンス情報検証部１３０より、検証失敗メッセージを返信されることにより、以下３つの不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ１７）。
【００４４】
・レスポンス情報の送信元端末は通信端末装置ＩＤ２ではない（通信端末装置ＩＤ２へのなりすまし攻撃が行われた）。
・通信端末装置ＩＤ１が不正な振る舞いを行った（通信端末装置ＩＤ１がチャレンジ情報Ｍを改竄して中継配送した疑いがある）。
・通信端末装置ＩＤ２が不正な振る舞いを行った。
【００４５】
一方、検証結果成功メッセージを返信されることにより、不正端末推定処理部１４０は、レスポンス情報の送信元端末を通信端末装置ＩＤ２であると認証する。また、通信端末ＩＤ２には確かにチャレンジ情報Ｍが到達していることを知る（ステップＳ１６）。次に、不正端末装置推定部１４０は、通信端末装置ＩＤ２に受信生成情報の配送を依頼するために、受信生成情報再送依頼メッセージを生成し、送信部１６０へ与える（ステップＳ１８）。そして、受信生成情報検証部１５０より、受信生成情報が与えられるのを待つ（ステップＳ１９）。受信生成情報検証部１５０は、受信生成情報Ｇｉを受けて、Ｇｉを検証する（ステップＳ２０）。不正端末装置推定処理部１４０は、受信生成情報検証部１５０より認証子（Ｇ２）検証結果失敗メッセージを与えられることにより、以下の不正の可能性があることを検知する（ステップＳ２２）。
【００４６】
・通信端末装置ＩＤ１が不正な振る舞いを行った（通信端末装置ＩＤ１は不正に振る舞ったことを検知されるのを恐れ、通信端末装置ＩＤ２からの受信生成情報を改竄して中継配送した疑いがある）。
・通信端末装置ＩＤ２が不正な振る舞いを行った。
・受信生成情報の送信元端末は通信端末装置ＩＤ２ではない（通信端末装置ＩＤ２へのな

りすまし攻撃が行われた）。

【００４７】

そして、受信生成情報検証部１５０より返信なしメッセージを与えられることにより、以下の不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ２１）。

・通信端末装置ＩＤ１が不正な振る舞いを行った（通信端末装置ＩＤ１は不正に振る舞ったことを検知されるのを恐れ、受信生成情報再送依頼メッセージ、もしくは、受信生成情報の中継を拒否した疑いがある）。

・通信端末装置ＩＤ２が不正な振る舞いを行った（通信端末装置ＩＤ２は不正に振る舞ったことを検知されるのを恐れ、受信生成情報の再送依頼を破棄した疑いがある）。

【００４８】

一方、不正端末装置推定部１４０は、受信生成情報検証部１５０より受信生成情報と、認証子（Ｇ２）検証成功メッセージを与えられることで、受信生成情報の検証処理を行う（ステップＳ２３）。受信生成情報の検証処理では、不正端末装置１００は、通信端末装置ＩＤ１より既に受信済みの、通信端末装置ＩＤ２より受信したレスポンス情報に含まれる情報（…，ＩＤ３，ＩＤ２，Ｆ２，Ｇ２）が、受信生成情報に含まれる情報と一致しているか否かを検証する（ステップＳ２４）。検証に失敗することで、以下の不正の可能性があることを検知し、不正端末装置推定処理を終了する（ステップＳ２６）。

【００４９】

・通信端末装置ＩＤ１が不正な振る舞いを行った（通信端末装置ＩＤ１はレスポンス情報を中継時に改竄した疑いがある）。

・通信端末装置ＩＤ２が不正な振る舞いを行った（通信端末装置ＩＤ２はレスポンス情報を中継時に改竄した疑いがある）。

【００５０】

一方、検証に成功することで、受信生成情報に含まれる情報のうち、「通信端末装置ＩＤ３から受信したレスポンス情報」が間違っていることを知る（ステップＳ２５）。次に、レスポンス情報を次に中継配送した通信端末装置ＩＤ３に関しても不正端末推定処理を行ってゆく（ステップＳ１４）。以上の不正端末推定処理が繰り返される。

【００５１】

以上のように、本実施形態によれば、Ｆｉを検証することにより送信元端末を確認する。また、Ｇｉを検証することにより受信生成情報が改竄されているか否かを確認する。図４及び図５のフローチャートに示されるように、Ｆｉ、Ｇｉの検証は、不正端末推定装置１００に近い側の通信端末装置ＩＤｉから順次に行われる。

【００５２】

図６は、本実施形態における通信端末装置ＩＤｉの内部構成を示すブロック図である。図６において、通信端末装置ＩＤｉは、チャレンジ情報格納部２１０、通信端末情報格納部２２０、レスポンス情報格納部２３０、受信証明情報生成部２４０、認証子生成部２５０、受信生成情報格納部２６０、レスポンス情報生成部２７０、送信部２８０及び受信部２９０を有する。

【００５３】

チャレンジ情報格納部２１０は、受信部２４０より与えられたチャレンジ情報Ｍを格納するものである。チャレンジ情報格納部２１０は、保持するチャレンジ情報Ｍを受信証明情報生成部２４０へ与える。

【００５４】

通信端末情報格納部２２０は、自身の識別子（ＩＤｉ）と鍵情報（ＫＩＤｉ）を保持するものである。通信端末情報格納部２２０は、保持する識別子と鍵情報を、受信証明情報生成部２４０と、認証子生成部２５０へ与える。

【００５５】

レスポンス情報格納部２３０は、受信部２９０より他の通信端末装置ＩＤｉのレスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）を与えられることにより、当該

レスポンス情報に含まれる、レスポンス情報の配送中継に関わった全通信端末の識別子（…，ＩＤ(ｉ＋１)）を受信証明情報識別子へ、また、与えられたレスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）を認証子生成部２５０へ与えるものである。

【００５６】

受信証明情報生成部２４０は、チャレンジ情報生成部２１０より与えられたチャレンジ情報Ｍと、通信端末情報格納部２２０より与えられた自身の識別子（ＩＤｉ）と鍵情報（ＫＩＤｉ）と、レスポンス情報格納部２３０より与えられた識別子（…，ＩＤ(ｉ＋１)）より、認証子（Ｆｉ）（式１を参照）を生成するものである。ただし、レスポンス情報の返信を自身がトリガとなって開始する場合には、上記識別子（…，ＩＤ(ｉ＋１)）はレスポンス情報格納部より与えられなくても良い。受信証明情報生成部２４０は、生成した認証子（Ｆｉ）を認証子生成部２５０へ与える。

【００５７】

認証子生成部２５０は、レスポンス情報格納部２３０より与えられたレスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）と、通信端末情報格納部２２０より与えられた自身の識別子（ＩＤｉ）と鍵情報（ＫＩＤｉ）と、受信証明情報生成部２４０より与えられた認証子（Ｆｉ）より、認証子（Ｇｉ）（式２を参照）を生成するものである。認証子生成部２５０は、上記レスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）と、自身の識別子（ＩＤｉ）と、認証子（Ｆｉ）と、生成した認証子（Ｇｉ）を受信生成情報格納部２６０へ与える。ただし、レスポンス情報の返信を自身がトリガとなって開始する場合には、上記レスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）はレスポンス情報格納部２３０より与えられなくても良いし、受信生成情報格納部２６０へ与えなくても良い。

【００５８】

受信生成情報格納部２６０は、認証子生成部２５０より与えられた、レスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）と、自身の識別子（ＩＤｉ）と、認証子（Ｆｉ）と、認証子（Ｇｉ）を保持するものである。ただし、レスポンス情報の返信を自身がトリガとなって開始する場合には、上記レスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）は認証子生成部２５０より与えられなくても良い。受信生成情報格納部２６０は、上記与えられた情報のうち、レスポンス情報の識別子（…，ＩＤ(ｉ＋１)）と、自身の識別子（ＩＤｉ）と、認証子（Ｆｉ）と、認証子（Ｇｉ）をレスポンス情報生成部２７０へ与える。また、受信生成情報格納部２６０は、受信部２９０より受信生成情報再送依頼メッセージを与えられることにより、保持する受信生成情報へ与える。

【００５９】

レスポンス情報生成部２７０は、受信生成情報格納部２６０より、レスポンス情報の識別子（…，ＩＤ(ｉ＋１)）と、自身の識別子（ＩＤｉ）と、認証子（Ｆｉ）と、認証子（Ｇｉ）を与えられることにより、レスポンス情報（…，ＩＤ(ｉ＋１)，ＩＤｉ，Ｆｉ，Ｇｉ）を生成し、生成したレスポンス情報を送信部２８０へ与える。ただし、レスポンス情報の返信を自身がトリガとなって開始する場合には、上記レスポンス情報（…，ＩＤ(ｉ＋１)，Ｆ(ｉ＋１)，Ｇ(ｉ＋１)）は受信生成情報格納部２６０より与えられなくても良い。

【００６０】

送信部２８０は、レスポンス情報生成部２７０より与えられたレスポンス情報を不正端末推定装置１００へ配送（もしくは配送依頼）する。また、受信生成情報格納部２６０より与えられた受信生成情報を不正端末推定装置１００へ配送（もしくは配送依頼）する。

【００６１】

受信部２９０は、与えられたチャレンジ情報Ｍをチャレンジ情報格納部２１０へ与える。また、他の通信端末装置ＩＤ(ｉ＋１)より配送依頼を受けたレスポンス情報を、レスポンス情報格納部２３０へ与える。また、不正端末推定装置１００より与えられた受信生成情報再送依頼メッセージを、受信生成情報格納部へ与える。

【００６２】

次に、本実施形態の不正端末推定システムの動作を、図７から図１０を参照しながら説明する。ここで、本実施形態の鍵配送システムの動作は、大きくは、４段階の動作（Ｓ１０１，Ｓ１０２，Ｓ１０３，Ｓ１０４）で構成されている。

【００６３】

「第１段階Ｓ１０１（チャレンジ情報Ｍの配信）」

第１段階Ｓ１０１は、図７に示すように、以下の手順で行われる。

・不正端末推定装置１００が、チャレンジ情報生成部１１０にてチャレンジ情報Ｍを生成し、送信部１６０を通して通信端末装置ＩＤｉへ配送する。

・通信端末装置ＩＤｉは、受信部２９０を通してチャレンジ情報Ｍを受信し、チャレンジ情報格納部２１０で保持する。

【００６４】

「第２段階Ｓ１０２（レスポンス情報の返信）」

第２段階Ｓ１０２は、図８に示すように、以下の手順で行われる。

・通信端末装置ＩＤ３が、受信証明情報生成部２４０において認証子Ｆ３を生成する。さらに、認証子生成部２５０において認証子Ｇ３を生成する。通信端末装置ＩＤ３は、生成した情報（ＩＤ３，Ｆ３，Ｇ３）を受信生成情報格納部２６０に保持し、次にレスポンス情報生成部２７０においてレスポンス情報（ＩＤ３，Ｆ３，Ｇ３）を生成し、送信部２８０を通して不正端末推定装置１００へ送信する。

・通信端末装置ＩＤ２のレスポンス情報格納部２３０に、通信端末装置ＩＤ３が送信したレスポンス情報（ＩＤ３，Ｆ３，Ｇ３）が与えられる。通信端末装置ＩＤ２は、受信証明情報生成部２４０において認証子Ｆ２を生成する。さらに、認証子生成部２５０において認証子Ｇ２を生成する。通信端末装置ＩＤ２は、通信端末装置ＩＤ３から受信したレスポンス情報と生成した情報を受信生成情報（ＩＤ３，Ｆ３，Ｇ３，ＩＤ２，Ｆ２，Ｇ２）として受信生成情報格納部２６０に保持し、次にレスポンス情報生成部２７０においてレスポンス情報（ＩＤ３，ＩＤ２，Ｆ２，Ｇ２）を生成し、送信部２８０を通して不正端末推定装置１００へ送信する。

・通信端末装置ＩＤ１のレスポンス情報格納部２３０に、通信端末装置ＩＤ２が送信したレスポンス情報（ＩＤ３，ＩＤ２，Ｆ２，Ｇ２）が与えられる。通信端末装置ＩＤ１は、受信証明情報生成部２４０において認証子Ｆ１を生成する。さらに、認証子生成部２５０において認証子Ｇ１を生成する。通信端末装置ＩＤ１は、通信端末装置ＩＤ２から受信したレスポンス情報と生成した情報を受信生成情報（ＩＤ３，ＩＤ２，Ｆ２，Ｇ２，ＩＤ１，Ｆ１，Ｇ１）として受信生成情報格納部２６０に保持し、次にレスポンス情報生成部２７０においてレスポンス情報（ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１）を生成し、送信部２８０を通して不正端末推定装置１００へ送信する。

【００６５】

「第３段階Ｓ１０３（レスポンス情報の検証）」

第３段階Ｓ１０３は、図９に示すように、以下の手順で行われる。

・不正端末推定装置１００は、レスポンス情報を受信し、レスポンス情報検証部１３０においてレスポンス情報に含まれる認証子Ｇ１を検証する。検証に成功することで、チャレンジ情報Ｍが、レスポンス情報に含まれる識別子が示す通信端末装置ＩＤｉに正しく届いたことを知る。検証に失敗した場合は、不正端末装置推定処理を開始する（Ｓ１０４へ）。

【００６６】

「第４段階Ｓ１０４（不正端末推定処理の実行）」

第４段階Ｓ１０４は、図１０に示すように、以下の手順で行われる。

・不正端末推定装置１００は、不正端末装置推定処理部１４０において、不正端末装置推定処理を開始する。ここでは、図４、５に示すフローチャートに従って、不正端末を推定する。

・レスポンス情報検証部１３０において、レスポンス情報の送信元端末の検証（認証子Ｆｉの検証）を行う。

・受信生成情報検証部１５０において、通信端末より受信した受信生成情報の改竄チェック（認証子Ｇｉの検証）を行う

上述したように、Ｆｉ、Ｇｉの検証は、不正端末推定装置１００に近い側の通信端末装置ＩＤｉから順次に行われる。

【００６７】

本実施形態によれば、マルチホップネットワークを形成する通信端末装置ＩＤｉが、受信したチャレンジ情報に対するレスポンス情報を生成し、生成したレスポンス情報を不正端末推定装置１００に配送し、不正端末推定装置１００が、上記レスポンス情報が正当か否かを検証し、検証が失敗することで、レスポンス情報の配送に関わった通信端末装置ＩＤｉの中に不正に振る舞った通信端末装置ＩＤｉが存在することを判断し、不正端末推定装置１００が、上記各通信端末装置ＩＤｉに受信情報と生成情報の再送を依頼することによって、不正に振る舞った通信端末装置ＩＤｉを推定することが可能となる。

【００６８】

図７から１０に示した動作説明図において、通信端末装置ＩＤ２を不正端末装置とし、不正端末推定装置１００における不正端末推定処理の結果を、以下Ａ～Ｈの８パターンで例示する。以下のパターンＡ～Ｈでは、各ステップを図４及び図５のフローチャートの各ステップに対応させて説明する。

【００６９】

（パターンＡ）

通信端末装置ＩＤ２が、チャレンジ情報ＭをＭ’に改竄して、通信端末装置ＩＤ３へ中継配送した場合。

(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。

(b)不正端末推定装置１００は、Ｆ１の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Ｍが届けられたことがわかる。（ステップＳ１→Ｓ２→Ｓ３→）

(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（ステップＳ５→Ｓ６→）

(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（ステップＳ７→）

(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ１０→Ｓ１１→Ｓ１２→Ｓ１４→）

(f)不正端末推定装置１００は、Ｆ２の検証に成功し、レスポンス情報がＩＤ２を経由してきたことを知る。また、ＩＤ２に正しいチャレンジ情報Ｍが届けられたことがわかる。（ステップＳ１５→Ｓ１６→）

(g)不正端末推定装置１００は、通信端末装置ＩＤ２より受信生成情報を取得する。（ステップＳ１８→Ｓ１９→）

(h)不正端末推定装置１００は、受信生成情報のＧ２’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）

(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したＩＤ３，ＩＤ２，Ｆ２，Ｇ２’が、同じく通信端末装置ＩＤ２より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ２３→Ｓ２４→Ｓ２５→Ｓ１４→）

(j)不正端末推定装置１００は、Ｆ３の検証に失敗し、次の３つの可能性があることを推定する。（ステップＳ１５→Ｓ１７→）

・通信端末装置ＩＤ３が不正に振る舞った。

・通信端末装置ＩＤ２が不正に振る舞った。

・他の装置が通信端末装置ＩＤ３になりすましてレスポンス情報を返信した。
【００７０】
（パターンＢ）
通信端末装置ＩＤ２が、通信端末装置ＩＤ３から受信したレスポンス情報に含まれる通信端末装置ＩＤ３の識別子を改竄した場合（ＩＤ３→ＩＤ３’）
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１’の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Mが届けられたことがわかる。（ステップＳ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（ステップＳ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（ステップＳ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３’，ＩＤ２，ＩＤ１，Ｆ１’，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ１０→Ｓ１１→Ｓ１２→Ｓ１４）
(f)不正端末推定装置１００は、Ｆ２’の検証に成功し、レスポンス情報がＩＤ２を経由してきたことを知る。また、ＩＤ２に正しいチャレンジ情報Mが届けられたことがわかる。（ステップＳ１５→Ｓ１６→）
(g)不正端末推定装置１００は、通信端末装置ＩＤ２より受信生成情報を取得する。（ステップＳ１８→Ｓ１９→）
（受信生成情報として改竄前の識別子ＩＤ３を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したとされるレスポンス情報に含まれる識別子ＩＤ３が、同じく通信端末装置ＩＤ２より受信した受信生成情報に含まれる識別子ＩＤ３’と一致しないことを検出することで、次の可能性があることを推定する。（ステップＳ２３→Ｓ２４→Ｓ２６）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
（受信生成情報として改竄後の受信生成情報ＩＤ３’を送信した場合）：
(j)不正端末推定装置１００は、受信生成情報のＧ２’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(k)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したＩＤ３’，ＩＤ２，Ｆ２’，Ｇ２’が、通信端末装置ＩＤ２より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ２３→Ｓ２４→Ｓ２５→Ｓ１４→）
(l)不正端末推定装置１００は、Ｆ３’の検証に失敗し、次の３つの可能性があることを推定する。（ステップＳ１５→Ｓ１７）
・通信端末装置ＩＤ３が不正に振る舞った。
・通信端末装置ＩＤ２が不正に振る舞った。
・他の装置が通信端末装置ＩＤ３になりすましてレスポンス情報を返信した。
【００７１】
（パターンＣ）
通信端末装置ＩＤ２が、通信端末装置ＩＤ３から受信したレスポンス情報に含まれる認

証子Ｆ３を改竄した場合（Ｆ３→Ｆ３’）
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Ｍが届けられたことがわかる。（ステップＳ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（ステップＳ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（ステップＳ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ１０→Ｓ１１→Ｓ１２→Ｓ１４→）
(f)不正端末推定装置１００は、Ｆ２の検証に成功し、レスポンス情報がＩＤ２を経由してきたことを知る。また、ＩＤ２に正しいチャレンジ情報Ｍが届けられたことがわかる。（ステップＳ１５→Ｓ１６→）
(g)不正端末推定装置１００は、通信端末装置ＩＤ２より受信生成情報を取得する。（ステップＳ１８→Ｓ１９→）
（受信生成情報として改竄前の認証子Ｆ３を送信した場合）：
　（受信生成情報の認証子Ｇ２’をＧ２に生成し直して送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２の検証に成功することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したとされるレスポンス情報に含まれる認証子Ｇ２’が、通信端末装置ＩＤ２より受信した受信生成情報に含まれる認証子Ｇ２と一致しないことを検出することで、次の可能性があることを推定する。（ステップＳ２３→Ｓ２４→Ｓ２６→）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
（受信生成情報の認証子Ｇ２’を送信した場合）：
(j)不正端末推定装置１００は、受信生成情報のＧ２’の検証に失敗することで、次の可能性があることを推定する。（ステップＳ２０→Ｓ２２→）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすまして受信生成情報を返信した。
（受信生成情報として改竄後の受信生成情報Ｆ３’を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したＩＤ３，ＩＤ２，Ｆ２，Ｇ２’が、通信端末装置ＩＤ２より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ２３→Ｓ２４→Ｓ２５→Ｓ１４→）
(j)不正端末推定装置１００は、Ｆ３’を検証に失敗し、次の可能性があることを推定する。（ステップＳ１５→Ｓ１７）
・通信端末装置ＩＤ３が不正に振る舞った。
・通信端末装置ＩＤ２が不正に振る舞った。
・他の装置が通信端末装置ＩＤ３になりすましてレスポンス情報を返信した。

【００７２】
（パターンＤ）
通信端末装置ＩＤ２が、通信端末装置ＩＤ３から受信したレスポンス情報に含まれる認証子Ｇ３を改竄した場合（Ｇ３→Ｇ３’）
パターンＡの(a)～(f)まで同じ
(g)不正端末推定装置１００は、通信端末装置ＩＤ２より受信生成情報を取得する。（ステップＳ１８→Ｓ１９→）
（(g)で通信端末装置ＩＤ２が受信生成情報として改竄後の認証子Ｇ３’を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、ＩＤ３，ＩＤ２，Ｆ２，Ｇ２’が、通信端末装置ＩＤ２より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ２３→Ｓ２４→Ｓ２５→Ｓ１４→）
(j)不正端末推定装置１００は、Ｆ３の検証に成功し、レスポンス情報がＩＤ３を経由してきたことを知る。また、ＩＤ３に正しいチャレンジ情報Mが届けられたことがわかる。（ステップＳ１５→Ｓ１６→）
(k)不正端末推定装置１００は、通信端末装置ＩＤ３より受信生成情報を取得する。（ステップＳ１８→Ｓ１９→）
(l)不正端末推定装置１００は、受信生成情報のＧ３を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ３より送信されたことを確認する。
（ステップＳ２０→）
(m)不正端末推定装置１００は、通信端末装置ＩＤ２より受信した受信生成情報に含まれる、Ｇ３’が、通信端末装置ＩＤ３より受信した受信生成情報に含まれるＧ３と一致しないことを検出し、次の可能性があることを推定する。（ステップＳ２３→Ｓ２４→Ｓ２６）
・通信端末装置ＩＤ３が不正に振る舞った。
・通信端末装置ＩＤ２が不正に振る舞った。
（(g)で通信端末装置ＩＤ２が受信生成情報として改竄前の認証子Ｇ３を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２’の検証に失敗することで、次の可能性があることを推定する。（ステップＳ２０→Ｓ２２→）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすまして受信生成情報を返信した。
【００７３】
（パターンＥ）
通信端末装置ＩＤ２が、自身の識別子を偽った場合（ＩＤ２→ＩＤ２’）。
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１’の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Mが届けられたことがわかる。
（ステップＳ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（Ｓ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認す

る。（Ｓ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３，ＩＤ２’，ＩＤ１，Ｆ１’，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（Ｓ１０→Ｓ１１→Ｓ１２→Ｓ１４→）
(f)不正端末推定装置１００は、Ｆ２’の検証に失敗し、次の可能性があることを推定する。（Ｓ１５→Ｓ１７）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすましてレスポンス情報を返信した。
【００７４】
（パターンＦ）
通信端末装置ＩＤ２が、正当な認証子Ｆ２を付加しなかった場合（Ｆ２→Ｆ２’）
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Ｍが届けられたことがわかる。（Ｓ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（Ｓ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（Ｓ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（Ｓ１０→Ｓ１１→Ｓ１２→Ｓ１４→）
(f)不正端末推定装置１００は、Ｆ２’の検証に失敗し、次の可能性があることを推定する。（Ｓ１５→Ｓ１７→）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすましてレスポンス情報を返信した。
【００７５】
（パターンＧ）
通信端末装置ＩＤ２が、正当な認証子Ｇ２を付加しなかった場合（Ｇ２→Ｇ２’）
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Ｍが届けられたことがわかる。（Ｓ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（Ｓ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１’を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（Ｓ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ３，ＩＤ２，ＩＤ１，Ｆ１，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（Ｓ１０→Ｓ１１→Ｓ１２→Ｓ１４→）
(f)不正端末推定装置１００は、Ｆ２の検証に成功し、レスポンス情報がＩＤ２を経由してきたことを知る。また、ＩＤ２に正しいチャレンジ情報Ｍが届けられたことがわかる。（Ｓ１５→Ｓ１６→）

(g)不正端末推定装置１００は、通信端末装置ＩＤ２より受信生成情報を取得する。（Ｓ１８→Ｓ１９→）
（受信生成情報として改竄前の認証子Ｇ２を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２の検証に成功することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ２より送信されたことを確認する。（ステップＳ２０→）
(i)不正端末推定装置１００は、通信端末装置ＩＤ１より受信した受信生成情報に含まれる、通信端末装置ＩＤ２より受信したとされるレスポンス情報に含まれる認証子Ｇ２’が、通信端末装置ＩＤ２より受信した受信生成情報に含まれる認証子Ｇ２と一致しないことを検出することで、次の可能性があることを推定する。（ステップＳ２３→Ｓ２４→Ｓ２６）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
（受信生成情報として改竄後の認証子Ｇ２’を送信した場合）：
(h)不正端末推定装置１００は、受信生成情報のＧ２’の検証に失敗することで、次の可能性があることを推定する。（ステップＳ２０→Ｓ２２）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすまして受信生成情報を返信した。

【００７６】

（パターンＨ）
通信端末装置ＩＤ２が、レスポンス情報を配送中継した通信端末装置の識別子を削除した場合（レスポンス情報からＩＤ３を削除）
(a)不正端末推定装置１００は、Ｇ１’の検証に失敗し、不正端末推定処理を開始する。
(b)不正端末推定装置１００は、Ｆ１’の検証に成功し、レスポンス情報がＩＤ１を経由してきたことを知る。また、ＩＤ１に正しいチャレンジ情報Ｍが届けられたことがわかる。
（ステップＳ１→Ｓ２→Ｓ３→）
(c)不正端末推定装置１００は、通信端末装置ＩＤ１より受信生成情報を取得する。（ステップＳ５→Ｓ６→）
(d)不正端末推定装置１００は、受信生成情報のＧ１´を検証することにより、受信生成情報が中継途中で改竄されることなく、通信端末装置ＩＤ１より送信されたことを確認する。（ステップＳ７→）
(e)不正端末推定装置１００は、通信端末装置ＩＤ１より受信したレスポンス情報ＩＤ２，ＩＤ１，Ｆ１’，Ｇ１’が、同じく通信端末装置ＩＤ１より受信した受信生成情報に含まれる情報と一致するかどうかを確認する。（ステップＳ１０→Ｓ１１→Ｓ１２→Ｓ１４→）
(f)不正端末推定装置１００は、Ｆ２の検証に失敗し、次の可能性があることを推定する。（ステップＳ１５→Ｓ１７）
・通信端末装置ＩＤ２が不正に振る舞った。
・通信端末装置ＩＤ１が不正に振る舞った。
・他の装置が通信端末装置ＩＤ２になりすましてレスポンス情報を返信した。

【００７７】

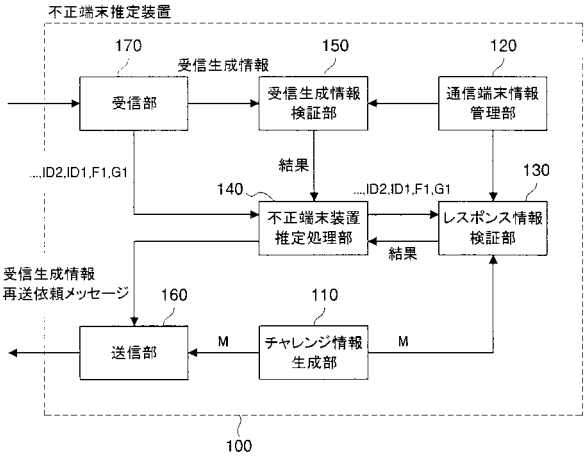
以上説明したように本実施形態によれば、正当だと認識している通信端末装置が不正に振る舞ったときに、不正に振る舞った通信端末装置がどの装置であるかを推定することが可能となる。従って、ネットワークに認証済みの正当な通信端末装置が、攻撃者に鍵情報を不正に入手されることにより、不正に振る舞うという脅威が存在する場合に、これら不正に振る舞った通信端末装置を推定することができる。これにより、例えば、不正な通信端末装置であると推定された通信端末装置をネットワークから切り離すといった処理が可能となる。

【００７８】
一方、本発明の別の効果として、不正端末推定装置１００が、レスポンス情報の検証に成功することで、チャレンジ情報Ｍがレスポンス情報の配送中継に関わった全ての通信端末装置（レスポンス情報に含まれる識別子が示す通信端末装置）に正しく届けられたことがわかる。例えば、チャレンジ情報として、ネットワーク内の通信端末装置に正しく届けたい重要なメッセージを設定することで、その重要なメッセージが確実に通信端末装置に届いたことを確認することができる。
【００７９】
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。
【００８０】
上記各実施形態の説明においても、種々変形実施形態に言及したが、さらに以下に例示するような変形実施形態を挙げることができる。
【００８１】
例えば、レスポンス情報の検証に失敗した複数の経路に関して、それぞれ不正端末装置推定処理を行い、その推定結果の統計情報から不正端末装置を推定してもよい。
【００８２】
また、レスポンス情報が配送中継された経路を不正端末推定装置１００が完全に把握しているときは、レスポンス情報には当該レスポンス情報の配送に関わった通信端末装置ＩＤｉの識別子を必ずしも含めなくても良い。
【００８３】
不正端末推定装置１００は、チャレンジ情報を配送せず、他の装置がチャレンジ情報を配送しても良い。不正端末推定装置１００は、配信されたチャレンジ情報を別途の手段で安全に入手できれば良い。
【００８４】
マルチホップのネットワーク構造については特に限定しない。ツリー型ネットワークであってもよいし、メッシュ型ネットワークであっても良い。
【００８５】
レスポンス情報を配送中継する経路は、特に限定しない。通信端末装置ＩＤｉが保持するルーティングテーブルに従っても良いし、ランダムに決定しても良い。また、不正端末推定装置１００がなんらかの方法で指定してもよい。環状になっていても良いし、任意のノードを重複しても良い。また、レスポンス情報は、任意の通信端末装置ＩＤｉから複数の経路で返信されても良い。
【図面の簡単な説明】
【００８６】
【図１】本発明の一実施形態における不正端末推定装置の内部構成を示すブロック図である。
【図２】通信端末装置より不正端末推定装置へ返信されるレスポンス情報の一例を示す模式図である。
【図３】受信生成情報の一例を示す模式図である。
【図４】不正端末推定処理の手順を示すフローチャートである。
【図５】図４に続いて、不正端末推定処理の手順を示すフローチャートである。
【図６】本実施形態における通信端末装置ＩＤｉの内部構成を示すブロック図である。
【図７】本実施形態の不正端末推定システムの動作を示す模式図である。
【図８】本実施形態の不正端末推定システムの動作を示す模式図である。
【図９】本実施形態の不正端末推定システムの動作を示す模式図である。
【図１０】本実施形態の不正端末推定システムの動作を示す模式図である。
【符号の説明】

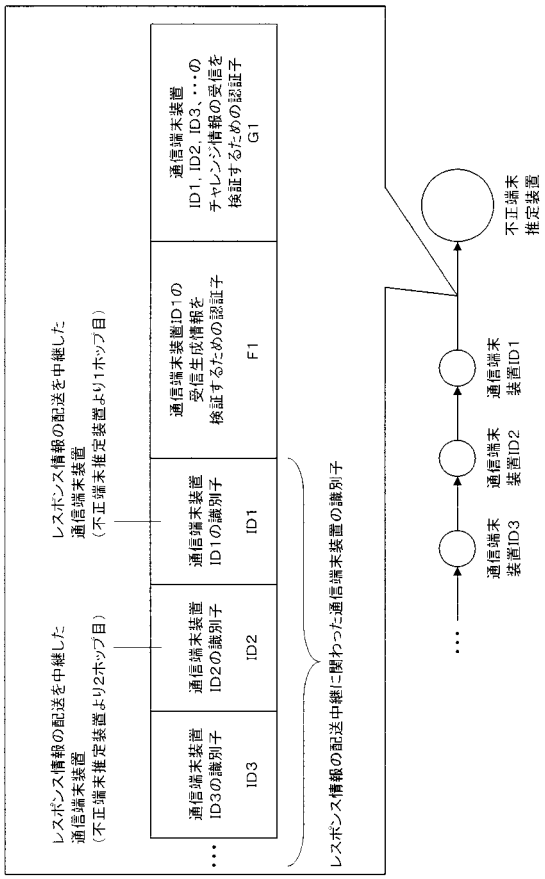
【００８７】

１００　不正端末推定装置
１２０　通信端末情報管理部
１３０　レスポンス情報検証部
１４０　不正端末装置推定処理部
１６０　送信部
１７０　受信部
２３０　レスポンス情報格納部
２５０　認証子生成部
２６０　受信生成情報格納部
２８０　送信部
２９０　受信部

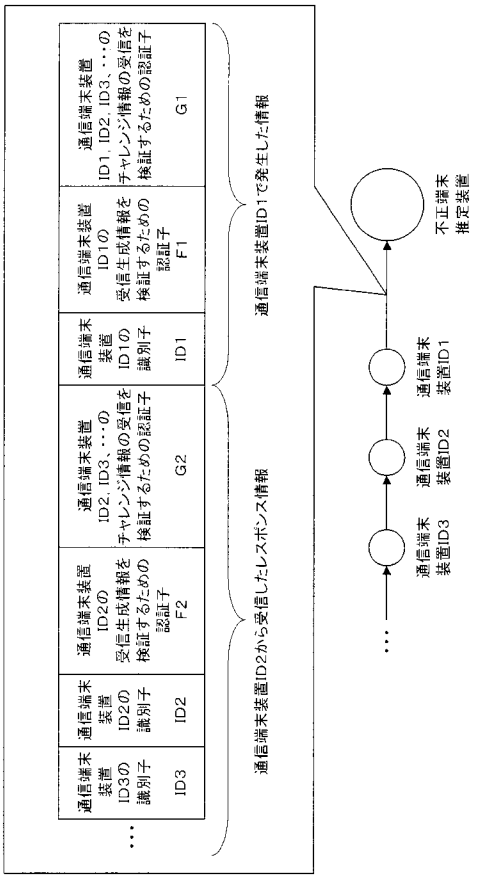
【図１】



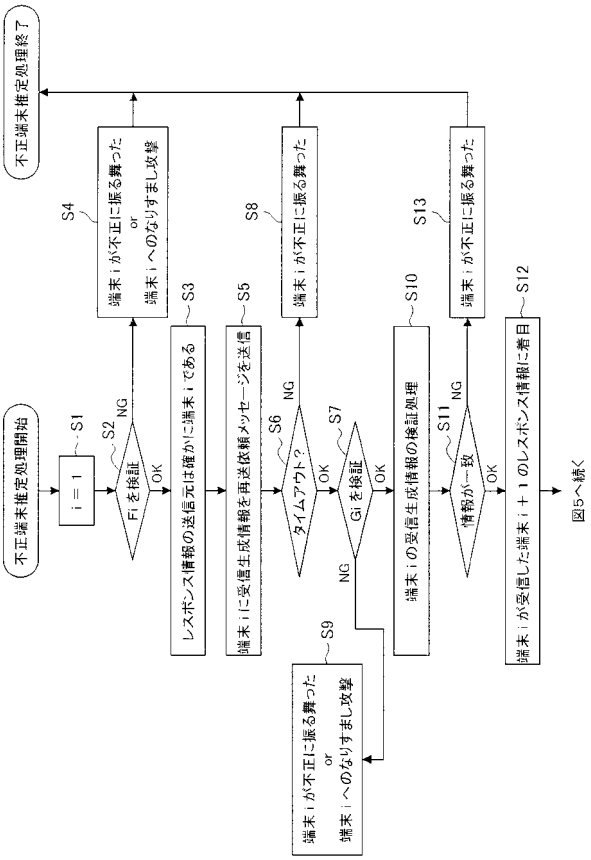
【図２】



【図３】


通信端末装置ID3の識別子 ID3
通信端末装置ID2の識別子 ID2
通信端末装置ID2の受信生成情報を検証するための認証子 F2
通信端末装置 ID2, ID3, …のチャレンジ情報の受信を検証するための認証子 G2
通信端末装置ID1の識別子 ID1
通信端末装置 ID1の受信生成情報を検証するための認証子 F1
通信端末装置 ID1, ID2, ID3, …のチャレンジ情報の受信を検証するための認証子 G1
通信端末装置ID2から受信したレスポンス情報
通信端末装置ID1で発生した情報
通信端末装置ID3
通信端末装置ID2
通信端末装置ID1
不正端末推定装置

【図４】


不正端末推定処理開始
i = 1
S1
Fi を検証
S2
NG
OK
端末 i が不正に振る舞った or 端末 i へのなりすまし攻撃
S4
レスポンス情報の送信元は確かに端末 i である
S3
端末 i に受信生成情報を再送依頼メッセージを送信
S5
タイムアウト？
S6
NG
OK
端末 i が不正に振る舞った
S8
Gi を検証
S7
NG
OK
端末 i が不正に振る舞った or 端末 i へのなりすまし攻撃
S9
端末 i の受信生成情報の検証処理
S10
情報が一致
S11
NG
OK
端末 i が不正に振る舞った
S13
端末 i が受信した端末 i + 1 のレスポンス情報に着目
S12
不正端末推定処理終了
図5へ続く

【図５】

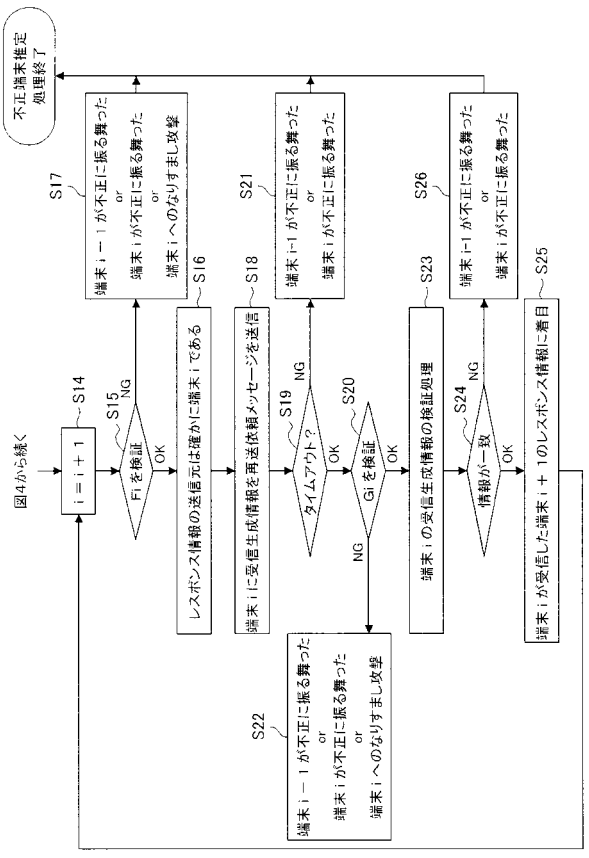
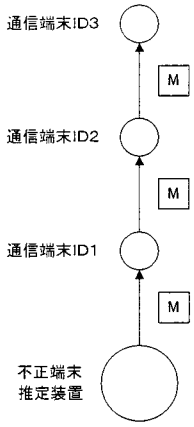


図4から続く
i = i + 1
S14
Fi を検証
S15
NG
OK
端末 i − 1 が不正に振る舞った or 端末 i が不正に振る舞った or 端末 i へのなりすまし攻撃
S17
レスポンス情報の送信元は確かに端末 i である
S16
端末 i に受信生成情報を再送依頼メッセージを送信
S18
タイムアウト？
S19
NG
OK
端末 i-1 が不正に振る舞った or 端末 i が不正に振る舞った
S21
Gi を検証
S20
NG
OK
端末 i − 1 が不正に振る舞った or 端末 i が不正に振る舞った or 端末 i へのなりすまし攻撃
S22
端末 i の受信生成情報の検証処理
S23
情報が一致
S24
NG
OK
端末 i-1 が不正に振る舞った or 端末 i が不正に振る舞った
S26
端末 i が受信した端末 i + 1 のレスポンス情報に着目
S25
不正端末推定処理終了

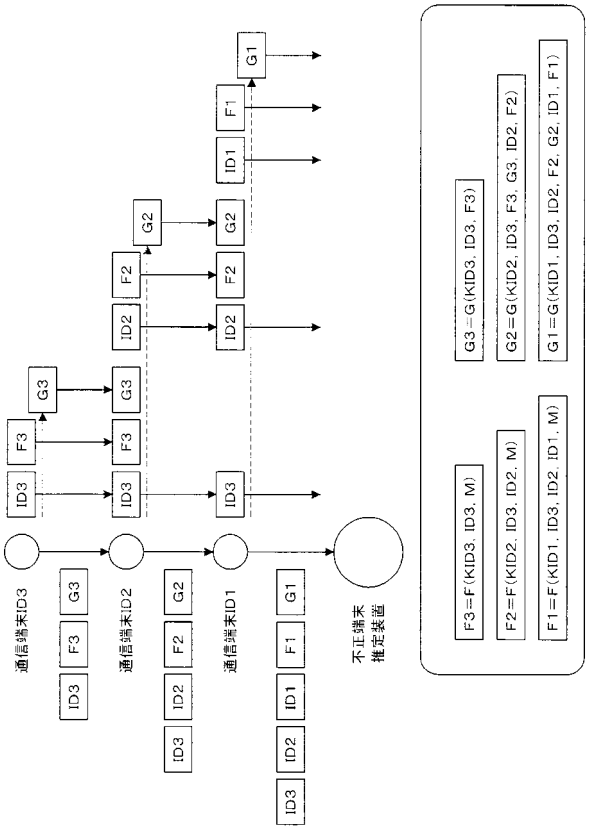
【図６】

200
通信端末装置
受信部
290
M
チャレンジ情報格納部
210
M
レスポンス情報格納部
230
受信証明情報生成部
240
IDi,KIDi
通信端末情報管理部
220
認証子生成部
250
Fi
IDi,KIDi
受信生成情報格納部
260
情報生成情報再送依頼メッセージ
...IDi+1,Fi+1,Gi+1,IDi,Fi,Gi
...IDi+1,Fi+1,Gi+1
...IDi+1,Fi+1,Gi+1
...IDi+1,IDi,Fi,Gi
レスポンス情報生成部
270
送信部
280
...IDi+1,IDi,Fi,Gi

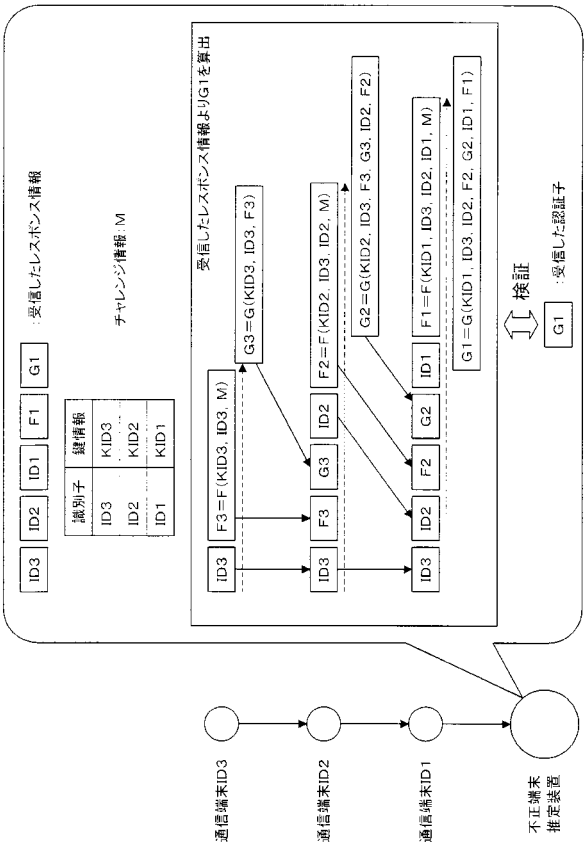
【図７】


通信端末ID3
通信端末ID2
通信端末ID1
不正端末
推定装置
M
M
M

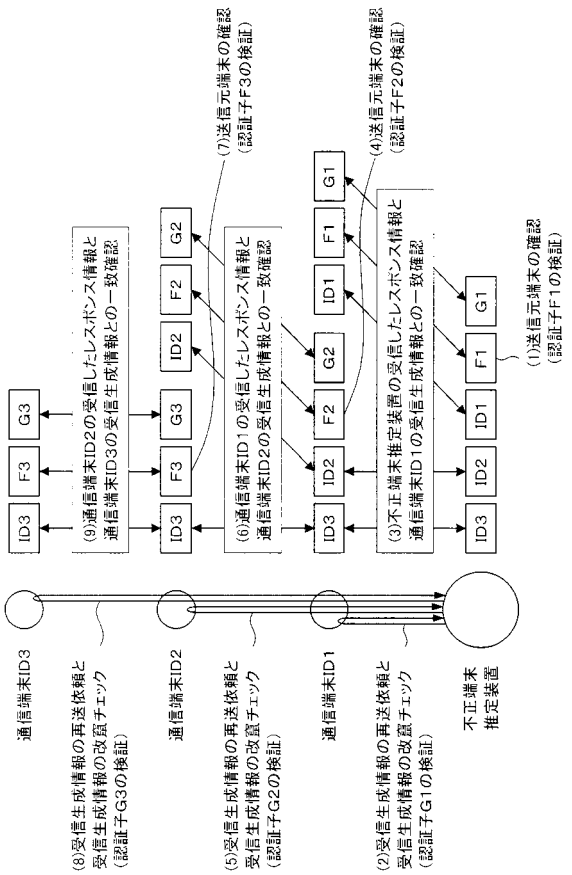
【図８】


通信端末ID3
通信端末ID2
通信端末ID1
不正端末
推定装置
F3=F(KID3, ID3, M)
F2=F(KID2, ID3, ID2, M)
F1=F(KID1, ID3, ID2, ID1, M)
G3=G(KID3, ID3, F3)
G2=G(KID2, ID3, F3, G3, ID2, F2)
G1=G(KID1, ID3, ID2, F2, G2, ID1, F1)

【図９】


ID3
ID2
ID1
F1
G1
：受信したレスポンス情報
識別子
鍵情報
ID3
KID3
ID2
KID2
ID1
KID1
チャレンジ情報：M
受信したレスポンス情報よりG1を算出
F3=F(KID3, ID3, M)
G3=G(KID3, ID3, F3)
F2=F(KID2, ID3, ID2, M)
G2=G(KID2, ID3, F3, G3, ID2, F2)
F1=F(KID1, ID3, ID2, ID1, M)
G1=G(KID1, ID3, ID2, F2, G2, ID1, F1)
検証
G1
：受信した認証子
通信端末ID3
通信端末ID2
通信端末ID1
不正端末
推定装置

【図１０】


通信端末ID3
通信端末ID2
通信端末ID1
不正端末
推定装置
(1)送信元端末の確認
(認証子F1の検証)
(2)受信生成情報の再送依頼と
受信生成情報の改竄チェック
(認証子G1の検証)
(3)不正端末推定装置の受信したレスポンス情報と
通信端末ID1の受信生成情報との一致確認
(4)送信元端末の確認
(認証子F2の検証)
(5)受信生成情報の再送依頼と
受信生成情報の改竄チェック
(認証子G2の検証)
(6)通信端末ID1の受信したレスポンス情報と
通信端末ID2の受信生成情報との一致確認
(7)送信元端末の確認
(認証子F3の検証)
(8)受信生成情報の再送依頼と
受信生成情報の改竄チェック
(認証子G3の検証)
(9)通信端末ID2の受信したレスポンス情報と
通信端末ID3の受信生成情報との一致確認

フロントページの続き

(56)参考文献　特開２００５－２８６９５６（ＪＰ，Ａ）
特開２００６－１５７８５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２