(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 8 月 9 日(09.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/104977 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04W 84/18* (2009.01)
H04W 84/12 (2009.01) *H04W 88/08* (2009.01)

(21) 国際出願番号: PCT/JP2011/051964

(22) 国際出願日: 2011 年 1 月 31 日(31.01.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社(**FUJITSU LIMITED**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 古川　和快 (**FURUKAWA, Kazuyoshi**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内 Kanagawa (JP). 伊豆　哲也(**IZU, Tetsuya**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内 Kanagawa (JP). 兒島　尚 (**KOJIMA, Hisashi**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内 Kanagawa (JP). 武仲　正彦 (**TAKENAKA, Masahiko**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内 Kanagawa (JP).

(74) 代理人: 酒井　昭徳(**SAKAI, Akinori**); 〒1006020 東京都千代田区霞が関３丁目２番５号　霞が関ビルディング２０階　酒井総合特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

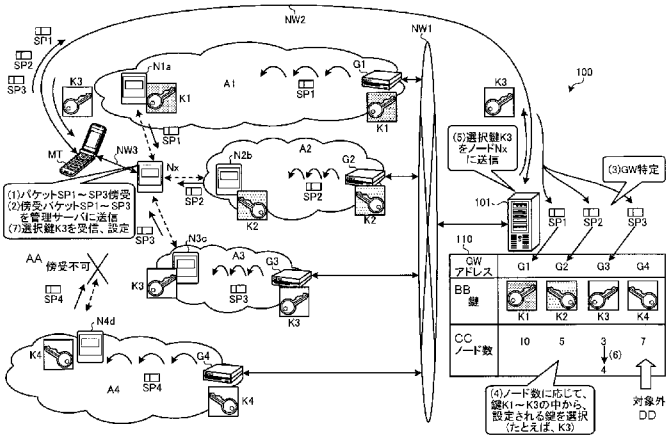
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,

[続葉有]

(54) **Title**: KEY SETTING METHOD, NODE, SERVER, AND NETWORK SYSTEM

(54) 発明の名称 : 鍵設定方法、ノード、サーバおよびネットワークシステム

[図1]



(1) Intercept packets (SP1-SP3).
(2) Send intercepted packets (SP1-SP3) to management server.
(3) Specify gateways.
(4) Select key to be set (e.g., K3), from keys (K1-K3) according to number of nodes.
(5) Send selection key (K3) to node (Nx).
(7) Receive and set selection key (K3).
110 Gateway address
AA Intercept not possible.
BB Key
CC Number of nodes
DD Not included.

(57) **Abstract**: A new node (Nx) sends intercepted encrypted packets (SP1-SP3) to a management server (101) via a mobile terminal (MT). Once the management server (101) receives the encrypted packets (SP1-SP3) from the new node (Nx), the management server (101) specifies the gateway (G1-G3) addresses contained therein. The management server (101) selects a selection key to be set to the new node (Nx), from among encryption keys (K1-K3) associated with the gateway (G1-G3) addresses. Specifically, the management server (101) determines the selection key based on the number of nodes in ad hoc networks (A1-A3) to which the gateways (G1-G3) belong. The management server (101) sends the selection key (K3) to the new node (Nx) via the mobile terminal (MT). The new node (Nx) receives the selection key (K3) and sets same as the key to encrypt the packets or to decode the encrypted packets.

(57) 要約:　新規ノード（Ｎｘ）は、傍受した暗号化パケット（ＳＰ１～ＳＰ３）を携帯端末（ＭＴ）経由で管理サーバ（１０１）に送信する。管理サーバ（１０１）は、新規ノード（Ｎｘ）から暗号化パケット（ＳＰ１～ＳＰ３）を受信すると、それらに含まれているゲートウェイ（Ｇ１～Ｇ３）のアドレスを特定する。管理サーバ（１０１）は、ゲートウェイ（Ｇ１～Ｇ３）のアドレスに関連付けられている暗号鍵（Ｋ１～Ｋ３）の中から、新規ノード（Ｎｘ）に設定させる選択鍵を選択する。具体的には、ゲートウェイ（Ｇ１～Ｇ３）が所属するアドホックネットワーク（Ａ１～Ａ３）のノード数により、選択鍵を決定する。管理サーバ（１０１）は、選択鍵（Ｋ３）を携帯端末（ＭＴ）を介して新規ノード（Ｎｘ）に送信する。新規ノード（Ｎｘ）は、選択鍵（Ｋ３）を受信して、パケットを暗号化、または、暗号化パケットを復号するための鍵に設定する。

WO 2012/104977 A1

GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

鍵設定方法、ノード、サーバおよびネットワークシステム

技術分野

[0001]　本発明は、データを暗号化するための鍵を設定する鍵設定方法、ノード、サーバおよびネットワークシステムに関する。

背景技術

[0002]　アドホックネットワークは、無線通信でリンクする自己構成型のネットワークの一種である。アドホックネットワークは複数のノードにより構成される。また、アドホックネットワーク内の各ノードは、マルチホップ通信によりパケットの送受信をおこなう。マルチホップ通信は、互いの通信圏内に存在しないノード同士が、各ノードの通信圏内に存在する別のノードを介して通信をおこなう技術である。

[0003]　また、アドホックネットワークとインターネット、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの他のネットワークとを接続する場合、ゲートウェイと呼ばれる中継機器を用いて、ネットワーク間の通信の転送が行われる。

[0004]　アドホックネットワークを利用した技術として、各家庭の電力メータに無線通信可能なノードを組み込んで、作業員が現地に出向くことなく、アドホックネットワーク経由でメータ確認などの業務をおこなうシステムがある。各家庭の電力の使用量などの個人情報を扱うアドホックネットワークでは、秘匿性や改ざん防止の観点からセキュアな通信をおこなうことが要求される。

[0005]　そこで、従来のシステムでは、アドホックネットワーク内のノード間で送受信されるパケットを暗号化することで、セキュアな通信を確保することが行われている。この際、システム内の全ノードで共通の暗号鍵を用いた場合、鍵漏洩時のリスクが大きいため、ゲートウェイごとに暗号鍵を変えるシス

テムがある。

[0006] また、システムへの新規ノードの初期導入時などにおいて、新規ノードは、暗号鍵が設定されるまでの間、アドホックネットワーク内の他のノードとセキュアな通信をおこなうことができない。このため、アドホックネットワーク経由で新規ノードに暗号鍵を自動設定することが難しく、作業員が現地に出向いて暗号鍵の設定作業を行っている。

[0007] また、セキュア通信に関する先行技術として、たとえば、ブロードキャストにより通信をおこなうネットワークの暗号鍵を管理する技術がある（たとえば、下記特許文献１参照。）。また、アドホックネットワークにおいて通信開始時の鍵交換を安定しておこなうための技術がある（たとえば、下記特許文献２参照。）。また、アドホックネットワーク内の各ノードが適応ゲートウェイを選択するための技術がある（たとえば、下記特許文献３参照。）。

先行技術文献

特許文献

[0008] 特許文献1：特開２００３－３４８０７２号公報

特許文献2：特開２００７－８８７９９号公報

特許文献3：特開２００９－８１８５４号公報

発明の概要

発明が解決しようとする課題

[0009] しかしながら、上述した従来技術では、アドホックネットワーク内の各ノードに設定する暗号鍵をゲートウェイごとに変える場合、新規ノードの初期導入時などにおいて、新規ノードが属するゲートウェイを特定することが難しいという問題があった。たとえば、新規ノードの設置場所の住所から候補となるゲートウェイを絞り込むことはできても、天候や近傍の建物との位置関係などの要因により通信状況が変化する。このため、実際にどのゲートウェイと通信可能であるかを作業員が現地に出向いて確認する必要があり、作

業員の暗号鍵の設定作業にかかる作業時間および作業負荷の増大を招くという問題がある。

[0010] また、新規ノードが複数のアドホックネットワークと通信可能である場合、いずれかのアドホックネットワークにも所属することになる。しかしながら、各アドホックネットワーク間でノード数に差があると、たとえば、ノード数が多いアドホックネットワークでは、通信負荷が増大するといった通信負荷のばらつきが生じ、通信の安定性を欠くという問題がある。

[0011] また、ノード数が多いアドホックネットワークのゲートウェイに障害が発生すると、ゲートウェイと通信ができなくなるノード数も多くなるため、複数のアドホックネットワーク全体で見た場合、通信の安定性を欠くという問題がある。

[0012] また、上述したように、新規ノードが実際にどのゲートウェイと通信可能であるかを作業員が現地に出向いて確認できたとしても、そのアドホックネットワークのノード数まではわからない。したがって、作業員が、複数のアドホックネットワークのノード数が均等になるように新規ノードを導入するのは非常に困難であり、結局、作業員の暗号鍵の設定作業にかかる作業時間および作業負荷の増大を招くという問題がある。

[0013] 本発明は、上述した従来技術による問題点を解消するため、アドホックネットワーク内のノードが用いる暗号鍵の設定作業の効率化を図ることができる鍵設定方法、ノード、サーバ、およびネットワークシステムを提供することを目的とする。また、複数のアドホックネットワーク間のノードの平均化を図ることにより通信の安定化を図ることができる鍵設定方法、ノード、サーバおよびネットワークシステ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

[0014] 上述した課題を解決し、目的を達成するため、本願の一観点によれば、アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークからのパケットを受信可能なノードが、前記複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用い

て暗号化された複数の暗号化パケットを、前記複数のアドホックネットワークから受信し、前記アドホックネットワーク群の各アドホックネットワーク内のゲートウェイ固有の鍵およびノード数を保持するサーバと通信可能な携帯端末との接続を検知し、前記携帯端末との接続が検知された場合、前記携帯端末を介して、受信された前記複数の暗号化パケットを前記サーバに送信し、前記携帯端末を介して、前記複数のアドホックネットワークの中で前記ノード数が最大ではないいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を前記サーバから受信し、受信された鍵を、前記いずれかのアドホックネットワーク内でマルチホップ通信させるパケットを暗号化するための鍵に設定する鍵設定方法、ノード、およびネットワークシステムを提供することができる。

[0015] また、本願の一観点によれば、アドホックネットワーク群の各ゲートウェイと通信可能であり、前記各ゲートウェイのアドレスと、前記各ゲートウェイ固有の鍵と、前記アドホックネットワーク群の各アドホックネットワーク内に存在するノード数と、を記憶するデータベースを有するサーバが、前記アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを受信したノードから、当該ノードに接続された携帯端末を介して、前記複数の暗号化パケットを受信し、受信された前記複数の暗号化パケットの各暗号化パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定し、前記複数のアドホックネットワークのうち、特定されたノード数のうち最大でないいずれかのノード数であるいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を、前記データベースにおいて前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択し、選択された選択鍵を、前記携帯端末を介して、前記ノードに送信する鍵設定方法、サーバおよびネットワークシステムを提供することができる。

発明の効果

[0016] 本鍵設定方法、ノード、サーバおよびネットワークシステムによれば、アドホックネットワーク内のノードが用いる暗号鍵の設定作業の効率化を図ることができるという効果を奏する。また、複数のアドホックネットワーク間のノードの平均化を図ることにより通信の安定化を図ることができるという効果を奏する。

図面の簡単な説明

[0017] [図1]図１は、実施の形態にかかるネットワークシステムでのノード数平均化例を示す説明図である。

[図2]図２は、実施の形態にかかるネットワークシステムの一実施例を示す説明図である。

[図3]図３は、実施の形態にかかる管理サーバのハードウェア構成例を示すブロック図である。

[図4]図４は、実施の形態にかかるノード等のハードウェア構成例を示すブロック図である。

[図5]図５は、図１に示した暗号鍵ＤＢの記憶内容の一例を示す説明図である。

[図6]図６は、ネットワークシステムへの新規ノードの導入例を示す説明図である。

[図7]図７は、新規ノードの導入時におけるネットワークシステムの動作例（前半）を示すシーケンス図である。

[図8]図８は、新規ノードの導入時におけるネットワークシステムの動作例（後半）を示すシーケンス図である。

[図9]図９は、ノードの機能的構成例を示すブロック図である。

[図10]図１０は、暗号化パケットのデータ構造の一例を示す説明図である。

[図11]図１１は、管理サーバの機能的構成例を示すブロック図である。

[図12]図１２は、暗号化パケットのデータ構造の一例を示す説明図（その２）である。

[図13]図１３は、管理サーバの認証情報の一例を示す説明図である。

[図14]図１４は、携帯端末の認証情報の一例を示す説明図である。

[図15]図１５は、ノードの鍵設定処理手順の一例を示すフローチャートである。

[図16]図１６は、管理サーバの鍵提供処理手順の一例を示すフローチャートである。

[図17]図１７は、ステップＳ１６０２の鍵抽出処理（その１）の具体的な処理手順の一例を示すフローチャートである。

[図18]図１８は、ステップＳ１６０２の鍵抽出処理（その２）の具体的な処理手順の一例を示すフローチャートである。

発明を実施するための形態

[0018] 以下に添付図面を参照して、この発明にかかる鍵設定方法、ノード、サーバおよびネットワークシステムの実施の形態を詳細に説明する。

[0019] （ネットワークシステムでのノード数平均化例）

図１は、実施の形態にかかるネットワークシステムでのノード数平均化例を示す説明図である。本実施の形態のネットワークシステム１００では、管理サーバ１０１とインターネット、ＬＡＮ、ＷＡＮなどのネットワークＮＷ１を介して通信可能な複数のアドホックネットワーク（図１では、Ａ１～Ａ４の４個）の各ノード数の平均化を図る。具体的には、導入済みのノードの配置換えをおこなうのではなく、新規ノードＮｘの導入時に、ノード数が少ないアドホックネットワークに新規ノードＮｘを追加することで、段階的に平均化を図る。

[0020] ノード数の平均化を図ることで、通信負荷のばらつきの低減化を図り、また、ゲートウェイに障害が発生したときのリスク分散をおこなうことができるため、アドホックネットワークＡ１～Ａ４全体での通信の安定性の向上を図ることができる。以下、図１について詳細に説明する。

[0021] 管理サーバ１０１は、暗号鍵ＤＢ（データベース）１１０を備え、各ゲートウェイ固有の暗号鍵を管理するコンピュータである。図１では、管理サー

バ１０１は、ゲートウェイＧ１～Ｇ４に固有の暗号鍵Ｋ１～Ｋ４を、暗号鍵ＤＢ１１０に保持している。また、管理サーバ１０１は、ゲートウェイＧ１～Ｇ４が所属するアドホックネットワークＡ１～Ａ４のノード数を、暗号鍵ＤＢ１１０に保持している。図１では、アドホックネットワークＡ１のノード数は１０個、アドホックネットワークＡ２のノード数は５個、アドホックネットワークＡ３のノード数は３個、アドホックネットワークＡ４のノード数は７個である。

[0022] アドホックネットワークＡ１～Ａ４内のノードは、それぞれのゲートウェイＧ１～Ｇ４固有の暗号鍵Ｋ１～Ｋ４を有する。ゲートウェイＧ１～Ｇ４も、それぞれゲートウェイ固有の鍵Ｋ１～Ｋ４を有する。これにより、各アドホックネットワークＡ１～Ａ４では、それぞれの暗号鍵Ｋ１～Ｋ４を用いた暗号化パケット通信や暗号化パケットの復号をおこなうことができ、セキュアに通信をおこなうことができる。

[0023] また、各ゲートウェイＧ１～Ｇ４は、定期的に、配下のノード群に対し、それぞれ暗号鍵Ｋ１～Ｋ４で暗号化された暗号化パケットＳＰ１～ＳＰ４をブロードキャストする。暗号化パケットＳＰ１～ＳＰ４は、それぞれのアドホックネットワークＡ１～Ａ４内のノードの時刻同期や、マルチホップ通信の際のルーティングテーブルの更新などのために配信される。なお、暗号化パケットＳＰ１～ＳＰ４は、一時的に（不定期に）配信されてもよい。

[0024] ここで、新規ノードＮｘを導入する場合について説明する。図１では、新規ノードＮｘを設置した場合、アドホックネットワークＡ１～Ａ３の通信圏内にあり、アドホックネットワークＡ４の通信圏外にあるとする。新規ノードＮｘは、いずれの暗号鍵Ｋ１～Ｋ４も未設定であるため、暗号化パケットの送信や受信パケットの復号はできないが、パケットの単なる受信は可能である。

[0025] このように、復号ができないにもかかわらずパケットを受信することを、「傍受」と称す。また、傍受されたパケットについては、新規ノードＮｘはいずれの暗号鍵Ｋ１～Ｋ４も持っていないため復号できないが、破棄せずに

送信することもできることとする。なお、アドホックネットワークＡ１～Ａ４では、それぞれの暗号鍵Ｋ１～Ｋ４で暗号化されていないパケットは、受信しても破棄される。

[0026] 図１では、アドホックネットワークＡ１のノードＮ１ａ、アドホックネットワークＡ２のノードＮ２ｂ、アドホックネットワークＡ３のノードＮ３ｃにそれぞれ配信された暗号化パケットＳＰ１～ＳＰ３が、新規ノードＮｘに傍受されている。なお、アドホックネットワークＡ４のノードＮ４ｄは新規ノードＮｘの通信圏外であるため、暗号化パケットＳＰ４は傍受されない。

[0027] 新規ノードＮｘは、傍受した暗号化パケットＳＰ１～ＳＰ３を管理サーバ１０１に送ることで、どのアドホックネットワークＡ１～Ａ４に所属可能かを通知する必要がある。ただし、ノードＮｘが、暗号化パケットＳＰ１～ＳＰ３を送信元となるアドホックネットワークＡ１～Ａ３経由で管理サーバ１０１に送っても、送信元が新規ノードＮｘであると、管理サーバ１０１は特定できない。

[0028] また、暗号化パケットＳＰ１をアドホックネットワークＡ２に送るなど、異なるアドホックネットワークに送るとアドホックネットワーク内のノードが復号できない。すなわち、暗号化パケットＳＰ１は暗号鍵Ｋ１で暗号化されているため、アドホックネットワークＡ２内のノードが持つ暗号鍵Ｋ２では復号できない。したがって、アドホックネットワークとは別のネットワーク経由で、傍受した暗号化パケットＳＰ１～ＳＰ３を管理サーバ１０１に送信する。

[0029] 具体的には、管理サーバ１０１と通信可能な携帯端末ＭＴを新規ノードＮｘに接続する。これにより、ネットワークＮＷ３が設定される。また、携帯端末ＭＴと管理サーバ１０１とが接続されることで、携帯端末ＭＴと管理サーバ１０１間で通信が可能となる。これにより、ネットワークＮＷ２が設定される。

[0030] つぎに、ネットワークＮＷ２，ＮＷ３経由での暗号鍵設定処理手順について説明する。（１）まず、新規ノードＮｘは、暗号化パケットＳＰ１～ＳＰ

３を傍受する。暗号化パケットＳＰ４は通信圏外であるため、傍受できない。

[0031] （２）新規ノードＮｘは、傍受した暗号化パケットＳＰ１～ＳＰ３を携帯端末ＭＴ経由で管理サーバ１０１に送信する。

[0032] （３）管理サーバ１０１は、新規ノードＮｘから暗号化パケットＳＰ１～ＳＰ３を受信すると、暗号化パケットＳＰ１～ＳＰ３を解析して、暗号化パケットＳＰ１～ＳＰ３に含まれているゲートウェイＧ１～Ｇ３のアドレスを特定する。

[0033] （４）管理サーバ１０１は、（３）で特定されたゲートウェイＧ１～Ｇ３のアドレスに関連付けられている暗号鍵Ｋ１～Ｋ３の中から、新規ノードＮｘに設定させる暗号鍵（以下、「選択鍵」という）を選択する。具体的には、ゲートウェイＧ１～Ｇ３が所属するアドホックネットワークＡ１～Ａ３のノード数により、選択鍵を決定する。

[0034] たとえば、候補となる暗号鍵Ｋ１～Ｋ３のうち、最大ノード数以外のノード数となる暗号鍵Ｋ２，Ｋ３から選択する。この場合、最大ノード数でなければ、暗号鍵Ｋ２，Ｋ３のいずれでもよい。また、最小ノード数の暗号鍵Ｋ３としてもよい。図１では、暗号鍵Ｋ３が選択されたものとする。

[0035] （５）管理サーバ１０１は、選択鍵Ｋ３を、携帯端末ＭＴを介して新規ノードＮｘに送信する。

[0036] （６）そして、管理サーバ１０１は、暗号鍵Ｋ３に関連付けられているノード数を「３」から「４」に更新する。

[0037] （７）新規ノードは、管理サーバ１０１からの選択鍵Ｋ３を受信して、パケットを暗号化、または、暗号化パケットを復号するための鍵に設定する。

[0038] これにより、新規ノードＮｘは、アドホックネットワークＡ３に所属することとなり、アドホックネットワークＡ３内で暗号化通信が可能となる。このように、ノード数が少ないアドホックネットワークから新規ノードＮｘを導入することができるため、複数のアドホックネットワーク間でノード数の平均化を図ることができる。したがって、通信負荷のばらつきの低減化を図

り、また、ゲートウェイに障害が発生したときのリスク分散をおこなうことができることとなり、アドホックネットワークＡ１～Ａ４全体での通信の安定性の向上を図ることができる。

[0039] 以下、上述した図１に示したネットワークシステム１００でのノード数平均化例について具体的に説明する。

[0040] （ネットワークシステム１００の一実施例）

図２は、実施の形態にかかるネットワークシステム１００の一実施例を示す説明図である。図２において、ネットワークシステム１００は、管理サーバ１０１と、ゲートウェイＧ１～Ｇｎと、ノードＮ１－１～Ｎ１－ｍ１，…，Ｎｉ－１～Ｎｉ－ｍｉ，…，Ｎｎ－１～Ｎｎ－ｍｎと、を含む構成である。ｉはアドホックネットワークＡｉの数（ｉ＝１，２，…，ｎ），ｍｉは、アドホックネットワークＡｉ内のノード数である。

[0041] ネットワークシステム１００において、管理サーバ１０１とゲートウェイＧ１～Ｇｎは、インターネット、ＬＡＮ、ＷＡＮなどのネットワークＮＷ１を介して相互に通信可能に接続されている。また、ゲートウェイＧｉとノードＮｉ－１～Ｎｉ－ｍｉは、アドホックネットワークＡｉを介して接続されている。

[0042] ここで、管理サーバ１０１は、暗号鍵ＤＢ１１０を備え、各ゲートウェイＧ１～Ｇｎ固有の暗号鍵を管理するコンピュータである。ゲートウェイＧｉ固有の暗号鍵（以下、「暗号鍵Ｋｉ」という）は、ゲートウェイＧｉが属するアドホックネットワークＡｉ内のノード間で送受信されるパケットを暗号化するための鍵情報である。なお、暗号鍵ＤＢ１１０についての詳細な説明は後述する。

[0043] ゲートウェイＧｉは、アドホックネットワークＡｉとネットワークＮＷ１とを接続する中継機器である。ゲートウェイＧｉは、アドホックネットワークＡｉのプロトコルとネットワークＮＷ１のプロトコルの両方を理解し、アドホックネットワークＡｉとネットワークＮＷ１との間の通信の転送をおこなう。

[0044] また、ゲートウェイＧｉは、アドホックネットワークＡｉ内においてどのノードがどのノードに対し通信可能かを把握しており、この情報を元に、ゲートウェイＧｉは自律的にルーティングすることになる。各ノードＮｉ－１～Ｎｉ－ｍｉでは、ゲートウェイＧｉのルーティングにより、マルチホップ通信をおこなう際の転送元アドレスと転送先アドレスが設定されることとなる。この設定は、ゲートウェイＧｉからのブロードキャストパケットでおこなわれる。

[0045] ノードＮｉ－１～Ｎｉ－ｍｉは、所定の通信圏内の他ノードとマルチホップ通信をおこなう無線通信装置である。アドホックネットワークＡｉでは、すべてのノードＮｉ－１～Ｎｉ－ｍｉがゲートウェイＧｉと直接通信できる必要はなく、一部のノードがゲートウェイＧｉと通信可能であればよい。

[0046] そして、ノードＮｉ－１～Ｎｉ－ｍｉは、ゲートウェイＧｉからのブロードキャストパケットにより、パケットの転送元アドレスと転送先アドレスの組み合わせとなるルーティングテーブルを保持することとなる。なお、ルーティングテーブルがない場合でもマルチホップ通信が可能である。この場合、パケットには最大ホップ数が設定されているため、最大ホップ数を超えた以降は、転送されなくなる。

[0047] ネットワークシステム１００は、たとえば、各家庭の電力やガスの使用量を収集するシステムに適用することができる。具体的には、たとえば、各家庭の電力メータやガスメータに各ノードＮｉ－１～Ｎｉ－ｍｉを組み込むことで、アドホックネットワークＡｉ内のノード間で各家庭の電力やガスの使用量を送受信する。なお、各家庭の電力やガスの使用量は、各ノードＮｉ－１～Ｎｉ－ｍｉが計測してもよく、また、各ノードＮｉ－１～Ｎｉ－ｍｉが電力メータやガスメータから取得してもよい。

[0048] ゲートウェイＧｉは、アドホックネットワークＡｉ内のノードＮｉ－１～Ｎｉ－ｍｉから受信した各家庭の電力やガスの使用量を、ネットワークＮＷ１を介して電力会社やガス会社のサーバ（たとえば、管理サーバ１０１）に送信する。これにより、作業員が現地に出向くことなく電力やガスの使用量

を収集することができる。

[0049] また、ネットワークシステム１００では、アドホックネットワークＡｉごとにゲートウェイＧｉ固有の暗号鍵Ｋｉを用いてパケットを暗号化する。これにより、アドホックネットワークＡｉのセキュア通信（データ秘匿性、改ざん防止など）を確保する。また、アドホックネットワークＡｉごとに暗号鍵Ｋｉを変えることで、鍵漏洩時のリスクを低減させる。

[0050] なお、図２の例では、アドホックネットワークＡｉ内に１台のゲートウェイＧｉを設ける構成としたが、同一のアドホックネットワークＡｉ内に複数台のゲートウェイＧｉを設ける構成としてもよい。この場合、アドホックネットワークＡｉ内で送受信されるパケットを暗号化するための暗号鍵Ｋｉは、複数台のゲートウェイＧｉで共通である。

[0051] （管理サーバ１０１のハードウェア構成例）

図３は、実施の形態にかかる管理サーバ１０１のハードウェア構成例を示すブロック図である。図３において、管理サーバ１０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）３０１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３０２と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）３０３と、磁気ディスクドライブ３０４と、磁気ディスク３０５と、光ディスクドライブ３０６と、光ディスク３０７と、Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）３０８と、ディスプレイ３０９と、キーボード３１０と、マウス３１１と、を備えている。また、ＣＰＵ３０１～マウス３１１はバス３００によってそれぞれ接続されている。

[0052] ここで、ＣＰＵ３０１は、管理サーバ１０１の全体の制御を司る。ＲＯＭ３０２は、ブートプログラムなどのプログラムを記憶している。ＲＡＭ３０３は、ＣＰＵ３０１のワークエリアとして使用される。磁気ディスクドライブ３０４は、ＣＰＵ３０１の制御に従って磁気ディスク３０５に対するデータのリード／ライトを制御する。磁気ディスク３０５は、磁気ディスクドライブ３０４の制御で書き込まれたデータを記憶する。

[0053] 光ディスクドライブ３０６は、ＣＰＵ３０１の制御に従って光ディスク３

０７に対するデータのリード／ライトを制御する。光ディスク３０７は、光ディスクドライブ３０６の制御で書き込まれたデータを記憶したり、光ディスク３０７に記憶されたデータをコンピュータに読み取らせたりする。

[0054] Ｉ／Ｆ３０８は、通信回線を通じてネットワークＮＷ１，ＮＷ２に接続され、このネットワークＮＷ１，ＮＷ２を介して他の装置（たとえば、ゲートウェイＧｉ、携帯端末ＭＴ）に接続される。Ｉ／Ｆ３０８は、ネットワークＮＷ１，ＮＷ２と内部のインターフェースを司り、外部装置からのデータの入出力を制御する。Ｉ／Ｆ３０８には、たとえば、モデムやＬＡＮアダプタなどを採用することができる。

[0055] ディスプレイ３０９は、カーソル、アイコンあるいはツールボックスをはじめ、文書、画像、機能情報などのデータを表示する。このディスプレイ３０９は、たとえば、ＣＲＴ、ＴＦＴ液晶ディスプレイ、プラズマディスプレイなどを採用することができる。

[0056] キーボード３１０は、文字、数字、各種指示などの入力のためのキーを備え、データの入力をおこなう。また、タッチパネル式の入力パッドやテンキーなどであってもよい。マウス３１１は、カーソルの移動や範囲選択、あるいはウィンドウの移動やサイズの変更などをおこなう。ポインティングデバイスとして同様に機能を備えるものであれば、トラックボールやジョイスティックなどであってもよい。なお、携帯端末ＭＴについても、図３に示した管理サーバ１０１と同様のハードウェア構成により実現できる。

[0057] （ノード等のハードウェア構成例）

図４は、実施の形態にかかるノードのハードウェア構成例を示すブロック図である。図４において、ノードは、ＣＰＵ４０１と、ＲＡＭ４０２と、フラッシュメモリ４０３と、Ｉ／Ｆ４０４と、暗号化回路４０５と、を備えている。ＣＰＵ４０１～暗号化回路４０５は、バス４００によってそれぞれ接続されている。

[0058] ここで、ＣＰＵ４０１は、ノードの全体の制御を司る。ＲＡＭ４０２は、ＣＰＵ４０１のワークエリアとして使用される。フラッシュメモリ４０３は

、プログラムや暗号鍵などの鍵情報を記憶している。Ｉ／Ｆ４０４は、マルチホップ通信によりパケットを送受信する。また、ゲートウェイＧｉのＩ／Ｆ４０４は、通信回線を通じてネットワークＮＷ１に接続され、このネットワークＮＷ１を介して管理サーバ１０１に接続される。

[0059] 暗号化回路４０５は、データを暗号化する場合に暗号鍵によりデータを暗号化する回路である。暗号化をソフトウェア的に実行する場合は、暗号化回路４０５に相当するプログラムをフラッシュメモリ４０３に記憶させておくことで、暗号化回路４０５は不要となる。

[0060] （暗号鍵ＤＢ１１０の記憶内容）

図５は、図１に示した暗号鍵ＤＢ１１０の記憶内容の一例を示す説明図である。図５において、暗号鍵ＤＢ１１０は、ＩＤ、GWアドレスおよび暗号鍵のフィールドを有し、各フィールドに情報を設定することで、ゲートウェイＧ１～Ｇｎごとの鍵情報５００－１～５００－ｎをレコードとして記憶している。

[0061] ここで、ＩＤは、本明細書において説明上用いる各ゲートウェイＧｉの識別子である。GWアドレスは、ゲートウェイＧｉのアドレスである。GWアドレスとしては、たとえば、ゲートウェイＧｉのＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスやＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスを用いることができる。暗号鍵は、各ゲートウェイＧｉ固有の暗号鍵Ｋｉであり、具体的には、たとえば、１２８～２５６ビット程度のバイナリデータである。

[0062] 鍵情報５００－１を例に挙げると、ゲートウェイＧ１のGWアドレスは『ｘｘ：ｘｘ：ｘｘ：ｘｘ：１２：３４』、暗号鍵は『Ｋ１』である。なお、暗号鍵ＤＢ１１０は、たとえば、図３に示した管理サーバ１０１のＲＯＭ３０２、ＲＡＭ３０３、磁気ディスク３０５、光ディスク３０７などの記憶装置により実現される。

[0063] 暗号鍵ＤＢ１１０の記憶内容は、管理サーバ１０１がゲートウェイＧｉ固有の暗号鍵Ｋｉをゲートウェイ Ｇｉから受信することで更新してもよい。ま

た、図３に示したキーボード３１０やマウス３１１を用いたユーザの操作入力により、暗号鍵ＤＢ１１０の記憶内容を更新することにしてもよい。

[0064] （新規ノードＮの導入時における暗号鍵Ｋｉの設定例）

つぎに、ネットワークシステム１００への新規ノードの導入時における暗号鍵Ｋｉの設定例について説明する。

[0065] 図６は、ネットワークシステム１００への新規ノードの導入例を示す説明図である。図６において、ネットワークシステム１００の任意のアドホックネットワークＡｉ内に新規ノードＮｘが導入されている。なお、図６では、アドホックネットワークＡｉ内のノードＮｉ－１～Ｎｉ－ｍｉのうち、代表としてノードＮｉ－１～Ｎｉ－３を示している。

[0066] 新規ノードＮｘの導入時は、作業員ＯＰは新規ノードＮｘがどのアドホックネットワークＡｉに属しているのかわからない。そこで、本実施の形態では、作業員ＯＰが使用する携帯端末ＭＴを利用して、新規ノードＮｘがアドホックネットワークＡｉ内のノードＮｉ－ｘとして設定すべき暗号鍵Ｋｉを管理サーバ１０１に問い合わせる。そして、管理サーバ１０１が、暗号鍵Ｋｉを選択した場合、選択鍵Ｋｉを管理サーバ１０１から取得して新規ノードＮｉ－ｘに自動設定する。

[0067] ここで、携帯端末ＭＴは、作業員ＯＰが使用する携帯型の通信装置であり、たとえば、携帯電話機、ＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙ－ｐｈｏｎｅ　Ｓｙｓｔｅｍ）電話機、スマートフォン、ノート型のパーソナル・コンピュータなどである。携帯端末ＭＴは、直接通信できない新規ノードＮｘと管理サーバ１０１との間の通信を中継する。

[0068] 図７は、新規ノードＮｘの導入時におけるネットワークシステム１００の動作例（前半）を示すシーケンス図である。図７のシーケンスは、たとえば、作業員ＯＰが現地（新規ノードＮｘの設置場所）に出向くまでに行われる動作例である。

[0069] 図７のシーケンスにおいて、（１）ゲートウェイＧｉは、ゲートウェイＧｉ固有の暗号鍵Ｋｉを管理サーバ１０１に送信する。（２）管理サーバ１０

１は、ゲートウェイＧｉ固有の暗号鍵Ｋｉとゲートウェイ Ｇｉのアドレスとを関連付けて暗号鍵ＤＢ１１０に登録する。

[0070] （３）ゲートウェイＧｉは、ゲートウェイＧｉ固有の暗号鍵Ｋｉを用いて暗号化されたパケット（以下、「暗号化パケットＳＰｉ」という）をアドホックネットワークＡｉにブロードキャスト（同時通報）する。暗号化パケットＳＰｉには、たとえば、ゲートウェイＧｉのアドレスが含まれている。

[0071] （４）ノードＮｉ－１は、ゲートウェイＧｉからの暗号化パケットＳＰｉを通信圏内のノードＮｉ－３に送信する。（５）ノードＮｉ－３は、ノードＮｉ－１からの暗号化パケットＳＰｉを通信圏内の新規ノードＮｘに送信する。これにより、新規ノードＮｘは、暗号化パケットＳＰｉを傍受する。（６）新規ノードＮｘは、ノードＮｉ－３からの暗号化パケットＳＰｉを記録する。ただし、この時点では、新規ノードＮｘは、暗号鍵Ｋｉが未設定のため、暗号化パケットＳＰｉを復号することはできない。

[0072] なお、上述した（１）～（６）は、新規ノードＮｘと通信圏内にあるアドホックネットワークＡｉごとに実行される。したがって、通信圏内のアドホックネットワークＡｉが複数ある場合、新規ノードＮｘは暗号化パケットＳＰｉを通信圏内のアドホックネットワークＡｉごとに傍受することとなる。通信圏内のアドホックネットワークＡｉごとに傍受された暗号化パケットＳＰｉの集合を「暗号化パケット群ＳＰ」と称す。

[0073] 図８は、新規ノードＮｘの導入時におけるネットワークシステム１００の動作例（後半）を示すシーケンス図である。図８のシーケンスは、たとえば、作業員ＯＰが現地に出向いたあとに行われる動作例である。

[0074] 図８のシーケンスにおいて、（７）携帯端末ＭＴは、携帯電話網やインターネットなどのネットワークＮＷ２を介して管理サーバ１０１に接続する。この際、携帯端末ＭＴは、たとえば、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）を用いて、管理サーバ１０１とセキュアな通信をおこなう。なお、管理サーバ１０１と携帯端末ＭＴとの間でセキュア通信を実現するための通信方式については、図１３および図１４を用いて後述する。

[0075] （８）携帯端末ＭＴは、有線または無線のネットワークＮＷ３を介して新規ノードＮｘに接続する。具体的には、たとえば、作業員ＯＰが、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ケーブルを用いて、携帯端末ＭＴと新規ノードＮとを接続することで、携帯端末ＭＴと新規ノードＮとの間にネットワークＮＷ３が確立される。

[0076] （９）新規ノードＮｘは、ネットワークＮＷ３を介して、図７に示した（６）において記録した暗号化パケット群ＳＰを携帯端末ＭＴに送信する。

[0077] （１０）携帯端末ＭＴは、ネットワークＮＷ２を介して、新規ノードＮｘからの暗号化パケット群ＳＰを管理サーバ１０１に送信する。

[0078] （１１）管理サーバ１０１は、携帯端末ＭＴからの暗号化パケット群ＳＰの各々の暗号化パケットＳＰｉを解析して、各暗号化パケットＳＰｉに含まれているゲートウェイＧｉのアドレスから、新規ノードＮｘが通信可能なゲートウェイＧｉをそれぞれ特定する。

[0079] （１２）管理サーバ１０１は、（１１）で特定されたゲートウェイＧｉごとに、当該ゲートウェイＧｉのアドレスに関連付けられている暗号鍵Ｋｉを、暗号鍵ＤＢ１１０の中から抽出する。

[0080] （１３）管理サーバ１０１は、（１２）で抽出された各暗号鍵Ｋｉに関連付けられているノード数に応じて、新規ノードＮｘの設定対象となる暗号鍵を選択する。

[0081] （１４）管理サーバ１０１は、ネットワークＮＷ２を介して、選択鍵Ｋｓを携帯端末ＭＴに送信する。

[0082] （１５）携帯端末ＭＴは、ネットワークＮＷ３を介して、選択鍵Ｋｓを新規ノードＮｘに送信する。

[0083] （１６）新規ノードＮｘは、管理サーバ１０１からの選択鍵Ｋｓを受信して、パケットを暗号化、または、暗号化パケットを復号するための鍵に設定する。これにより、新規ノードＮｘは、選択鍵Ｋｓを有するゲートウェイＧｉが所属するアドホックネットワークＡｉに所属することとなる。すなわち、選択鍵Ｋｓ設定以降は、新規ノードＮｘは、アドホックネットワークＡｉ

内の一ノードとしてアドホックネットワークＡｉと同様にふるまうこととなる。

[0084] （１７）管理サーバ１０１は、選択鍵Ｋｓに関連付けられているノード数をインクリメント（＋１）する。これにより、新規ノードＮｘへの選択鍵Ｋｓ設定後におけるアドホックネットワークＡｉのノード数を参照することで、つぎに導入される新規ノードについても、図７および図８の（１）～（１７）と同様の処理を実行することができる。

[0085] なお、以下の説明において、「ノードＮ」とは、ネットワークシステム１００のアドホックネットワークＡ１～ＡｎのいずれかのアドホックネットワークＡｉ内でマルチホップ通信によりパケットを送受信するノード（新規ノードＮｘ含む。）を示す。また、「ノード等」とは、ネットワークシステム１００のゲートウェイＧ１～Ｇｎおよびノードを示す。

[0086] （ノードＮの機能的構成例）

図９は、ノードの機能的構成例を示すブロック図である。図９において、ノードＮは、パケット受信部９０１と、検知部９０２と、パケット送信部９０３と、鍵受信部９０４と、設定部９０５と、を含む構成である。

[0087] 各機能部（パケット受信部９０１～設定部９０５）は、具体的には、たとえば、図４に示したＲＡＭ４０２、フラッシュメモリ４０３などの記憶装置に記憶されたプログラムをＣＰＵ４０１に実行させることにより、または、Ｉ／Ｆ４０４により、その機能を実現する。また、各機能部（パケット受信部９０１～設定部９０５）の処理結果は、特に指定する場合を除いて、ＲＡＭ４０２、フラッシュメモリ４０３などの記憶装置に記憶される。

[0088] パケット受信部９０１は、アドホックネットワークＡｉ内からの暗号化パケットＳＰｉを受信する。暗号化パケットＳＰｉは、ゲートウェイＧｉ固有の暗号鍵Ｋｉを用いて暗号化されたパケットである。たとえば、暗号化パケットＳＰｉは、ゲートウェイＧｉ固有の暗号鍵Ｋｉで暗号化されたゲートウェイＧｉからのブロードキャストパケットである。ここで、暗号化パケットＳＰｉのデータ構造の一例について説明する。

[0089] 図１０は、暗号化パケットＳＰｉのデータ構造の一例を示す説明図である。図１０では、アドホックネットワークＡｉのゲートウェイＧｉからブロードキャストされた暗号化パケットＳＰ１を例に挙げている。図１０において、暗号化パケットＳＰｉは、ヘッダ部１０１０とペイロード部１０２０とを含む構成である。ヘッダ部１０１０には、宛先アドレス、差出アドレス、ホップ数およびGWアドレスが記述されている。ペイロード部１０２０には、暗号化されたデータ本体が記述されている（図１０中ハッチ部分）。

[0090] ここで、宛先アドレスは、送信先のアドレスである。ここでは、ブロードキャスト用のＭＡＣアドレス『００：００：００：００：００：００』が記述されている。差出アドレスは、転送元のアドレスである。ここでは、アドホックネットワークＡ１内のノードＮとは異なる他のノードＮのＭＡＣアドレスが記述されている。図１の例でいうと、暗号化パケットＳＰ１の転送元となるノードＮ１ａのＭＡＣアドレスが記述されることとなる。

[0091] ホップ数は、暗号化パケットＳＰｉを残り何回転送するのかを示す残余の転送回数である。すなわち、マルチホップの上限回数である。ゲートウェイＧｉからブロードキャストされる暗号化パケットＳＰｉのホップ数の最大値は予め設定されている。このホップ数は暗号化パケットＳＰｉの転送時にデクリメントされ、ホップ数が『０』となった暗号化パケットＳＰｉは棄却される。ここでは、暗号化パケットＳＰ１のホップ数『１０』が記述されているため、１０回マルチホップされると、その次はマルチホップされない。

[0092] GWアドレスは、暗号化パケットＳＰｉの送信元となるゲートウェイＧｉのアドレスである。ここでは、ゲートウェイＧ１のＭＡＣアドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：１２：３４』が記述されている。なお、ここでは宛先アドレス、差出アドレスおよびGWアドレスの一例として、ＭＡＣアドレスを用いて説明したが、ＩＰアドレスなどのアドレスを用いることにしてもよい。

[0093] また、ノードＮが暗号鍵Ｋｉ未設定の新規ノードＮｘである場合、パケット受信部９０１は、近隣ノードからの暗号化パケットＳＰｉを受信（傍受）

する。たとえば、パケット受信部９０１は、図１に示したように、アドホックネットワークＡ１～Ａ３からの暗号化パケットＳＰ１～ＳＰ３を傍受する。

[0094] また、パケット受信部９０１は、ノードＮに暗号鍵Ｋｉが設定されている場合であっても、通信圏内であれば暗号化パケットＳＰｉを傍受する。この場合、傍受したノードＮのルーティングテーブルでは、暗号化パケットＳＰの転送元が登録されていないため、傍受した暗号化パケットＳＰｉは、傍受したノードＮで破棄されることとなる。ルーティングテーブルがない場合は、ホップ数が０でない限り、他の近隣ノードに転送することになる。

[0095] 検知部９０２は、管理サーバ１０１と通信可能な携帯端末ＭＴとの接続を検知する。具体的には、たとえば、作業員ＯＰがＵＳＢケーブルを用いて携帯端末ＭＴと新規ノードＮとを接続した結果、検知部９０２が、ＵＳＢケーブルを介した携帯端末ＭＴとの接続を検知する。

[0096] パケット送信部９０３は、携帯端末ＭＴとの接続が検知された場合、携帯端末ＭＴを介して、受信（傍受）された暗号化パケット群ＳＰを管理サーバ１０１に送信する。具体的には、たとえば、パケット送信部９０３が、ＵＳＢケーブルなどのネットワークＮＷ３を介して、暗号化パケット群ＳＰを携帯端末ＭＴに送信する。この結果、携帯端末ＭＴが、ネットワークＮＷ２を介して、ノードＮからの暗号化パケット群ＳＰを管理サーバ１０１に送信する。

[0097] なお、暗号化パケットＳＰｉは同一のアドホックネットワークＡｉ内で複数の経路をたどって傍受されるため、同一の暗号化パケットＳＰｉは複数回受信される場合がある。この場合、複数個の同一暗号化パケットＳＰｉについては、１個だけ送信する。たとえば、図１の場合、暗号化パケットＳＰ１が６回、暗号化パケットＳＰ２が３回、暗号化パケットＳＰ３が１回受信されたとしても、暗号化パケットＳＰ１～ＳＰ３をそれぞれ１個送信することになる。これにより、暗号化パケット群ＳＰの通信負荷の低減化を図ることができる。

[0098] また、同一アドホックネットワークＡｉからの暗号化パケット数を、管理サーバ１０１での暗号鍵Ｋｉの選択基準とする場合は、パケット送信部９０３は、受信（傍受）された複数個の同一暗号化パケットＳＰｉを送信することとしてもよい。たとえば、図１の場合、暗号化パケットＳＰ１が６回、暗号化パケットＳＰ２が３回、暗号化パケットＳＰ３が１回受信されたとすると、ノードＮは、暗号化パケットＳＰ１を６個、暗号化パケットＳＰ２を３個、暗号化パケットＳＰ３を１個、管理サーバ１０１に送信することになる。

[0099] 鍵受信部９０４は、携帯端末ＭＴを介して、送信された暗号化パケット群ＳＰの中から管理サーバ１０１によって選択された選択鍵Ｋｓを、管理サーバ１０１から受信する。この選択鍵Ｋｓは、たとえば、ノードＮにおいてパケットを暗号化するとともに、暗号鍵Ｋｉを用いて暗号化された暗号化パケットＳＰｉを復号することができる共通鍵である。

[0100] 設定部９０５は、受信された選択鍵Ｋｓを、アドホックネットワークＡｉ内でマルチホップ通信させるパケットを暗号化するための鍵に設定する。具体的には、たとえば、設定部９０５は、特定の記憶領域に選択鍵Ｋｓを書き込む。特定の記憶領域のアドレスは、パケットを暗号化する際、または暗号化パケットＳＰｉを復号する際に指定されるアドレスである。これにより、以降においてノードＮが送信対象となるパケットを暗号化、および暗号化パケットＳＰｉを復号することが可能となり、アドホックネットワークＡｉ内のノード間でセキュア通信をおこなうことができる。

[0101] （管理サーバ１０１の機能的構成）

図１１は、管理サーバ１０１の機能的構成例を示すブロック図である。図１１において、管理サーバ１０１は、受信部１１０１と、抽出部１１０２と、送信部１１０３と、を含む構成である。各機能部（受信部１１０１～送信部１１０３）は、具体的には、たとえば、図３に示したＲＯＭ３０２、ＲＡＭ３０３、磁気ディスク３０５、光ディスク３０７などの記憶装置に記憶されたプログラムをＣＰＵ３０１に実行させることにより、または、Ｉ／Ｆ３

０８により、その機能を実現する。また、各機能部（受信部１１０１～送信部１１０３）の処理結果は、たとえば、ＲＡＭ３０３、磁気ディスク３０５、光ディスク３０７などの記憶装置に記憶される。

[0102] 受信部１１０１は、携帯端末ＭＴを介して、暗号化パケットＳＰｉをノードＮから受信する。具体的には、たとえば、受信部１１０１が、ネットワークＮＷ２を介して、ノードＮからの暗号化パケット群ＳＰを携帯端末ＭＴから受信する。

[0103] 抽出部１１０２は、暗号鍵ＤＢ１１０の中から、受信された暗号化パケットＳＰｉを復号するための暗号鍵Ｋｉを抽出する。具体的には、たとえば、抽出部１１０２が、暗号鍵ＤＢ１１０の中から、暗号化パケットＳＰｉに含まれるゲートウェイＧｉのアドレスと関連付けて記憶されている暗号鍵Ｋｉを抽出する。

[0104] たとえば、受信部１１０１によって図１０に示した暗号化パケットＳＰ１が受信されたとする。この場合、抽出部１１０２が、たとえば、暗号鍵ＤＢ１１０の中から、暗号化パケットＳＰ１に含まれるＧＷアドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：１２：３４』と関連付けて記憶されている暗号鍵Ｋ１を抽出する。ここで、抽出部１１０２についてより詳細に説明する。抽出部１１０２は、特定部１１２１と、復号部１１２２と、選択部１１２３と、を有する。

[0105] 特定部１１２１は、受信部１１０１によって受信された暗号化パケット群ＳＰの各暗号化パケットＳＰｉに含まれている各ゲートウェイＧｉのアドレスを特定する。そして、特定部１１２１は、特定された各ゲートウェイＧｉのアドレスに基づいて、各ゲートウェイＧｉが所属するアドホックネットワークＡｉ内に存在するノード数を特定する。具体的には、たとえば、特定部１１２１は、暗号化パケットＳＰｉのヘッダ部１０１０のＧＷアドレスに一致するＧＷアドレスと関連付けられているノード数を、暗号鍵ＤＢ１１０から抽出する。

[0106] たとえば、図１０の暗号化パケットＳＰ１では、ゲートウェイＧ１のＧＷ

アドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：１２：３４』が記述されているため、ゲートウェイＧ１のＧＷアドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：１２：３４』に関連付けられているノード数「１０」を、暗号鍵ＤＢ１１０から抽出する。

[0107] また、図１０に示した暗号化パケットＳＰ１のようにＧＷアドレスがヘッダ部１０１０に含まれていれば、上述したように、ＧＷアドレスを手掛かりに暗号鍵ＤＢ１１０の中からノード数や暗号鍵Ｋｉを抽出することができる。これに対して、ＧＷアドレスがペイロード部１０２０に含まれる場合がある。

[0108] 図１２は、暗号化パケットＳＰｉのデータ構造の一例を示す説明図（その２）である。図１２においても、図１０と同様、アドホックネットワークＡｉのゲートウェイＧｉからブロードキャストされた暗号化パケットＳＰ１を例に挙げる。

[0109] 図１２において、暗号化パケットＳＰｉは、ヘッダ部１２１０とペイロード部１２２０とを含む構成である。ヘッダ部１２１０には、宛先アドレス、差出アドレスおよびホップ数が記述されている。ペイロード部１２２０には、暗号化されたＧＷアドレスおよびデータ本体が記述されている（図１２中ハッチ部分）。

[0110] この場合、ＧＷアドレスを手掛かりに暗号鍵ＤＢ１１０の中からノード数や暗号鍵Ｋｉを抽出することはできない。そこで、復号部１１２２は、暗号鍵ＤＢ１１０に登録されている暗号鍵Ｋｉごとに、暗号鍵Ｋｉを用いて暗号化パケットＳＰｉの復号処理を実行する。これにより、抽出部１１０２は、暗号化パケットＳＰｉの復号に成功した暗号鍵Ｋｉを抽出することができる。

[0111] 復号の成否は、暗号化パケットＳＰｉを復号した復号後のパケットのフォーマットに基づいて判断することができる。具体的には、たとえば、抽出部１１０２は、復号部１１２２によって復号された復号後のパケットが、予め規定されたフォーマットのデータの場合、暗号化パケットＳＰｉの復号が成

功したと判断する。これにより、暗号化パケットＳＰｉのヘッダ部１２１０にＧＷアドレスが含まれていない場合であっても、暗号鍵ＤＢ１１０の中からノードＮに設定すべき適切な暗号鍵Ｋｉを抽出することができる。

[0112] 選択部１１２３は、特定部１１２１によって特定されたノード数のうち最大でないいずれかのノード数であるいずれかのアドホックネットワークＡｉ内のゲートウェイＧｉ固有の鍵を、暗号鍵ＤＢ１１０において複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する。具体的には、たとえば、特定部１１２１によりゲートウェイＧｉごとにノード数が特定されるため、選択部１１２３は、その中で最大ノード数以外のノード数のゲートウェイＧｉを選択する。そして、選択部１１２３は、選択されたゲートウェイＧｉのアドレスに関連付けられている暗号鍵Ｋｉを、暗号鍵ＤＢ１１０から抽出する。選択部１１２３によって暗号鍵ＤＢ１１０から抽出された暗号鍵Ｋｉが選択鍵Ｋｓとなる。

[0113] たとえば、図１に示したように、暗号化パケット群ＳＰが暗号化パケットＳＰ１～ＳＰ３である場合、ゲートウェイＧ１～Ｇ３に関連付けられているノード数１０個、５個、３個がそれぞれ特定される。選択部１１２３は、これらのノード数のうち最大ノード数である１０個以外の５個、３個に関連付けられているゲートウェイＧ２，Ｇ３を選択する。この場合、特定されたノード数のうち最小ノード数となる３個を選択するのが好ましい。ここでは、３個、すなわちゲートウェイＧ３が選択されたこととする。そして、選択部１１２３は、ゲートウェイＧ３に関連付けられている暗号鍵Ｋ３を選択鍵Ｋｓとして選択して、暗号鍵ＤＢ１１０から抽出する。

[0114] なお、選択部１１２３は、特定部１１２１によって特定されたノード数がいずれも同数である場合は、ランダムに選択してもよい。同様に、選択部１１２３は、特定部１１２１によって特定されたノード数のうち、最大ノード数以外の残余のノード数がいずれも同数である場合も、ランダムに選択してもよい。

[0115] また、同数の場合には、選択部１１２３は、傍受回数が最大の暗号化パケ

ットＳＰｉを配信したゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとしてもよい。すなわち、ノードＮは、同一暗号化パケットＳＰｉを複数回傍受し、それらをすべて管理サーバ１０１に送信する場合がある。たとえば、図１の場合、暗号化パケットＳＰ１が６回、暗号化パケットＳＰ２が３回、暗号化パケットＳＰ３が１回受信されたとすると、ノードＮは、暗号化パケットＳＰ１を６個、暗号化パケットＳＰ２を３個、暗号化パケットＳＰ３を１個、管理サーバ１０１に送信することになる。

[0116] ここで、アドホックネットワークＡ１～Ａ３のノード数がそれぞれ１０個である場合、同一ノード数となるため、選択部１１２３は、最大傍受回数（６回）であるアドホックネットワークＡ１のゲートウェイＧ１固有の暗号鍵Ｋ１を選択鍵Ｋｓとして抽出する。

[0117] 外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。したがって、傍受回数が最大のアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘは、最も安定性の高いアドホックネットワークＡｉで通信をおこなうことができる。

[0118] 一方、これとは逆に、傍受回数の少ないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることとしてもよい。たとえば、上述の例では、選択部１１２３は、最小傍受回数（１回）であるアドホックネットワークＡ３のゲートウェイＧ３固有の暗号鍵Ｋ３を選択鍵Ｋｓとして抽出する。

[0119] 外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。したがって、傍受回数が最小のアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘ導入の際、導入先のアドホックネットワークＡｉの通信経路を増強することができる。これにより、通信経路が少ないアドホックネ

ットワークＡｉでの通信の安定性の向上を図ることができる。

[0120] また、アドホックネットワークＡ２，Ａ３のノード数が、アドホックネットワークＡ１のノード数「１０個」よりも少ないが同数（たとえば、それぞれ４個）である場合、選択部１１２３は、最大傍受回数（３回）であるアドホックネットワークＡ２のゲートウェイＧ２固有の暗号鍵Ｋ２を選択鍵Ｋｓとして抽出する。

[0121] 外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。したがって、傍受回数が最大のアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘは、最も安定性の高いアドホックネットワークＡｉで通信をおこなうことができる。

[0122] 一方、これとは逆に、傍受回数の少ないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることとしてもよい。たとえば、上述の例では、選択部１１２３は、最小傍受回数（１回）であるアドホックネットワークＡ３のゲートウェイＧ３固有の暗号鍵Ｋ３を選択鍵Ｋｓとして抽出する。

[0123] 外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。したがって、傍受回数が少ないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘ導入の際、導入先のアドホックネットワークＡｉの通信経路を増強することができる。これにより、通信経路が少ないアドホックネットワークＡｉでの通信の安定性の向上を図ることができる。

[0124] なお、上述したノード数が同数の場合の選択方法は、ノード数が同数に限らず、ノード数に差があっても、その差があらかじめ設定しておいた許容範囲内であれば適用可能である。

[0125] 送信部１１０３は、携帯端末ＭＴを介して、選択鍵Ｋｓをノード Ｎに送信する。この結果、携帯端末ＭＴが、ネットワークＮＷ３を介して、管理サーバ１０１からの選択鍵Ｋｓをノード Ｎに送信する。

[0126] なお、上述した説明では、管理サーバ１０１が暗号化パケット群ＳＰを受信した時点において、暗号鍵ＤＢ１１０にゲートウェイＧｉ固有の暗号鍵Ｋｉが登録済みの場合を想定したが、これに限らない。たとえば、管理サーバ１０１が、暗号化パケットＳＰｉを受信したあとゲートウェイＧｉに問い合わせることで、選択部１１２３によって選択されたゲートウェイＧｉ固有の暗号鍵Ｋｉを取得することにしてもよい。これにより、ネットワークシステム１００内のすべてのゲートウェイＧ１～Ｇｎ固有の暗号鍵Ｋ１～Ｋｎを管理サーバ１０１が予め保持しておく必要がなくなる。

[0127] （管理サーバ１０１と携帯端末ＭＴとの間の通信方式）

ここで、管理サーバ１０１と携帯端末ＭＴとの間の通信方式の一実施例について説明する。まず、携帯端末ＭＴからみた管理サーバ１０１のサーバ認証について説明する。具体的には、たとえば、まず、携帯端末ＭＴが、予め決められたＩＰアドレスを用いて管理サーバ１０１に接続する。

[0128] そして、携帯端末ＭＴが、管理サーバ１０１からＳＳＬサーバ証明書を受信する。受信されたＳＳＬサーバ証明書は、たとえば、管理サーバ１０１のＩＰアドレスと関連付けて携帯端末ＭＴのＲＡＭ４０２やフラッシュメモリ４０３などの記憶装置に記憶される。

[0129] 図１３は、管理サーバ１０１の認証情報の一例を示す説明図である。図１３において、管理サーバ１０１の認証情報１３００は、ＩＰアドレスおよびＳＳＬサーバ証明書を有する。ＩＰアドレスは、管理サーバ１０１のＩＰアドレスである。Ｘ．５０９証明書は、管理サーバ１０１のＳＳＬサーバ証明書（公開鍵証明書）である。

[0130] 携帯端末ＭＴは、予め自端末ＭＴに組み込まれている公開鍵を用いて、ＳＳＬサーバ証明書を復号することでサーバ認証をおこなう。公開鍵は、たとえば、第三者認証機関によって発行されたものである。この公開鍵を用いて

ＳＳＬサーバ証明書を正しく復号できれば、ＳＳＬサーバ証明書が第三者認証機関によって証明された正しい証明書であることがわかり、ひいては管理サーバ１０１の身元が保証されたことになる。

[0131] つぎに、管理サーバ１０１からみた携帯端末ＭＴのユーザ認証について説明する。ここでは、図１４に示すような携帯端末ＭＴの認証情報１４００を用いて、携帯端末ＭＴのユーザ認証をおこなう場合を例に挙げて説明する。認証情報１４００は、たとえば、管理サーバ１０１のＲＯＭ３０２、ＲＡＭ３０３、磁気ディスク３０５、光ディスク３０７などの記憶装置に記憶されている。

[0132] 図１４は、携帯端末ＭＴの認証情報の一例を示す説明図である。図１４において、携帯端末ＭＴの認証情報１４００は、ユーザＩＤおよびパスワードを有する。ユーザＩＤは、携帯端末ＭＴの識別子である。パスワードは、携帯端末ＭＴを使用するユーザを認証するためのものである。

[0133] 具体的には、たとえば、まず、携帯端末ＭＴが、ユーザＩＤおよびパスワードのペアを管理サーバ１０１に送信する。このユーザＩＤおよびパスワードは、携帯端末ＭＴのフラッシュメモリ４０３に予め登録されていてもよく、また、携帯端末ＭＴの入力装置（不図示）を用いたユーザの操作入力により受け付けてもよい。

[0134] このあと、管理サーバ１０１は、携帯端末ＭＴからのユーザＩＤおよびパスワードのペアを、認証情報１４００のユーザＩＤおよびパスワードのペアと一致判定する。ここで、認証情報１４００のユーザＩＤおよびパスワードと一致すれば、携帯端末ＭＴのユーザの身元が保証されたことになる。

[0135] なお、認証後において、携帯端末ＭＴは、たとえば、管理サーバ１０１のＳＳＬサーバ証明書に含まれる公開鍵を用いてパケットを暗号化して管理サーバ１０１との通信をおこなう。これにより、管理サーバ１０１と携帯端末ＭＴとの間でセキュアな通信をおこなうことができる。

[0136] （ノードＮの鍵設定処理手順）

図１５は、ノードの鍵設定処理手順の一例を示すフローチャートである。

図１５のフローチャートにおいて、まず、ノードＮは、パケット受信部９０１により、アドホックネットワークＡｉ内のゲートウェイＧｉからブロードキャストされた暗号化パケットＳＰｉを受信したか否かを判断する（ステップＳ１５０１）。

[0137] ここで、暗号化パケットＳＰｉを受信するのを待って（ステップＳ１５０１：Ｎｏ）、受信した場合（ステップＳ１５０１：Ｙｅｓ）、ノードＮは、検知部９０２により、管理サーバ１０１と通信可能な携帯端末ＭＴとの接続を検知したか否かを判断する（ステップＳ１５０２）。

[0138] ここで、携帯端末ＭＴとの接続が検知されるのを待って（ステップＳ１５０２：Ｎｏ）、検知された場合（ステップＳ１５０２：Ｙｅｓ）、ノードＮは、パケット送信部９０３により、携帯端末ＭＴを介して、受信（傍受）された暗号化パケット群ＳＰを管理サーバ１０１に送信する（ステップＳ１５０３）。なお、暗号化パケット群ＳＰの送信は、一括しておこなってもよく、暗号化パケットＳＰｉが受信される都度、個別に送信してもよい。なお、送信可能な期間は、接続検知後、一定期間経過するまでとする。

[0139] なお、管理サーバ１０１が同一暗号化パケットＳＰｉの傍受回数を選択鍵Ｋｓの選択基準に利用する場合には、複数の同一暗号化パケットＳＰｉを暗号化パケット群ＳＰに含めて送信してもよい。たとえば、暗号化パケットＳＰ１について３回傍受した場合は、３個の暗号化パケットＳＰ１を暗号化パケット群ＳＰに含めることとなる。

[0140] また、管理サーバ１０１が同一暗号化パケットＳＰｉの傍受回数を選択鍵Ｋｓの選択基準に利用しない場合には、同一暗号化パケットＳＰｉについては１個のみ暗号化パケット群ＳＰに含めて送信してもよい。たとえば、暗号化パケットＳＰ１について３回傍受した場合でも、暗号化パケットＳＰ１については１個のみ暗号化パケット群ＳＰに含めることとなる。これにより、暗号化パケット群ＳＰの通信負荷の低減化を図ることができる。

[0141] これにより、同一暗号化パケットＳＰｉの傍受回数を、選択鍵Ｋｓの選択基準として管理サーバ１０１は利用することができる。したがって、傍受回

数が少ないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘ導入の際、導入先のアドホックネットワークＡｉの通信経路を増強することができる。これにより、通信経路が少ないアドホックネットワークＡｉでの通信の安定性の向上を図ることができる。

[0142] このあと、ノードＮは、鍵受信部９０４により、携帯端末ＭＴを介して、選択鍵Ｋｓを管理サーバ１０１から受信したか否かを判断する（ステップＳ１５０４）。

[0143] ここで、選択鍵Ｋｓを受信するのを待って（ステップＳ１５０４：Ｎｏ）、受信した場合（ステップＳ１５０４：Ｙｅｓ）、ノードＮは、設定部９０５により、受信された選択鍵Ｋｓを、パケットを暗号化するための鍵に設定して（ステップＳ１５０５）、本フローチャートによる一連の処理を終了する。

[0144] これにより、新規ノードＮｘは、選択鍵Ｋｓを共通鍵とするアドホックネットワークＡｉにおいてマルチホップ通信が可能となり、アドホックネットワーク間でノード数の平均化を図ることができる。

[0145] （管理サーバ１０１の鍵提供処理手順）

図１６は、管理サーバ１０１の鍵提供処理手順の一例を示すフローチャートである。図１６のフローチャートにおいて、まず、管理サーバ１０１は、受信部１１０１により、携帯端末ＭＴを介して、暗号化パケット群ＳＰをノードＮから受信したか否かを判断する（ステップＳ１６０１）。

[0146] ここで、暗号化パケット群ＳＰを受信するのを待って（ステップＳ１６０１：Ｎｏ）、受信した場合（ステップＳ１６０１：Ｙｅｓ）、管理サーバ１０１は、抽出部１１０２により、暗号鍵ＤＢ１１０の中から選択鍵Ｋｓを抽出する鍵抽出処理を実行する（ステップＳ１６０２）。そして、管理サーバ１０１は、送信部１１０３により、携帯端末ＭＴを介して、抽出された選択鍵ＫｓをノードＮに送信する（ステップＳ１６０３）。

[0147] また、管理サーバ１０１は、暗号鍵ＤＢ１１０において、選択鍵Ｋｓとな

った暗号鍵Ｋｉに関連付けられているノード数をインクリメント（＋１）して（ステップＳ１６０４）、本フローチャートによる一連の処理を終了する。

[0148] これにより、管理サーバ１０１は、新規ノードＮｘに、選択鍵Ｋｓを共通鍵とするアドホックネットワークＡｉにおいてマルチホップ通信をさせることが可能となり、アドホックネットワーク間でノード数の平均化を図ることができる。

[0149] ＜鍵抽出処理（その１）手順＞

つぎに、図１６に示したステップＳ１６０２の鍵抽出処理（その１）の具体的な処理手順について説明する。以下に説明する鍵抽出処理（その１）は、暗号化パケットＳＰｉに含まれるＧＷアドレスが暗号化されていない場合（図１０を参照）の処理である。

[0150] 図１７は、ステップＳ１６０２の鍵抽出処理（その１）の具体的な処理手順の一例を示すフローチャートである。図１７のフローチャートにおいて、まず、管理サーバ１０１は、抽出部１１０２により、図１６に示したステップＳ１６０１において受信された暗号化パケットＳＰｉに含まれるＧＷアドレスを特定する（ステップＳ１７０１）。

[0151] つぎに、管理サーバ１０１は、抽出部１１０２により、ゲートウェイＧｉの「ｉ」を「ｉ＝１」で初期化する（ステップＳ１７０２）。このあと、管理サーバ１０１は、抽出部１１０２により、暗号鍵ＤＢ１１０を参照して、ゲートウェイＧｉのＧＷアドレスを特定する（ステップＳ１７０３）。そして、管理サーバ１０１は、抽出部１１０２により、ステップＳ１７０１において特定されたＧＷアドレスと、ステップＳ１７０３において特定されたＧＷアドレスとが一致するか否かを判断する（ステップＳ１７０４）。

[0152] ここで、ＧＷアドレスが不一致の場合（ステップＳ１７０４：Ｎｏ）、管理サーバ１０１は、抽出部１１０２により、ゲートウェイＧｉの「ｉ」をインクリメントして（ステップＳ１７０５）、「ｉ」が「ｎ」より大きいか否かを判断する（ステップＳ１７０６）。ｎは、暗号鍵Ｋｉの総数（ゲートウ

ェイＧｉの総数）である。

[0153] ここで、「ｉ」が「ｎ」以下の場合（ステップＳ１７０６：Ｎｏ）、ステップＳ１７０３に戻る。一方、「ｉ」が「ｎ」より大きい場合（ステップＳ１７０６：Ｙｅｓ）、管理サーバ１０１は、別の暗号化パケットＳＰｉ（同一暗号化パケットＳＰｉではない）があるか否かを判断する（ステップＳ１７０７）。

[0154] 別の暗号化パケットＳＰｉがない場合（ステップＳ１７０７：Ｎｏ）、管理サーバ１０１は、ステップＳ１７１０で抽出済みの暗号鍵Ｋｉがあるか否かを判断する（ステップＳ１７０８）。抽出済みの暗号鍵Ｋｉがない場合（ステップＳ１７０８：Ｎｏ）、管理サーバ１０１は、抽出部１１０２により、エラー処理を実行して（ステップＳ１７０９）、管理サーバ１０１の一連の処理を終了する。

[0155] 一方、抽出済みの暗号鍵Ｋｉがある場合（ステップＳ１７０８：Ｙｅｓ）、管理サーバ１０１は、選択候補の各暗号鍵Ｋｉに関連付けられているノード数により、選択候補の各暗号鍵Ｋｉの中から、新規ノードＮｘに設定させる暗号鍵Ｋｉを選択鍵Ｋｓとして選択する（ステップＳ１７１２）。なお、上述したように、さらに、傍受回数を選択基準として用いてもよい。また、ステップＳ１７０７において、別の暗号化パケットＳＰｉがある場合（ステップＳ１７０７：Ｙｅｓ）、ステップＳ１７０１に戻る。

[0156] また、ステップＳ１７０４において、ＧＷアドレスが一致する場合（ステップＳ１７０４：Ｙｅｓ）、管理サーバ１０１は、抽出部１１０２により、暗号鍵ＤＢ１１０の中から暗号鍵Ｋｉおよび暗号鍵Ｋｉに関連付けられているノード数を抽出する（ステップＳ１７１０）。そして、管理サーバ１０１は、別の暗号化パケットＳＰｉ（同一暗号化パケットＳＰｉではない）があるか否かを判断する（ステップＳ１７１１）。

[0157] 別の暗号化パケットＳＰｉがある場合（ステップＳ１７１１：Ｙｅｓ）、ステップＳ１７０１に戻る。これにより、管理サーバ１０１は、ＧＷアドレスが一致する暗号鍵Ｋｉを選択候補として抽出することができる。

[0158] 一方、別の暗号化パケットＳＰｉがない場合（ステップＳ１７１１：Ｎｏ）、選択候補が抽出済みとなるため、管理サーバ１０１は、選択候補の各暗号鍵Ｋｉに関連付けられているノード数により、選択候補の各暗号鍵Ｋｉの中から、新規ノードＮｘに設定させる暗号鍵Ｋｉを選択鍵Ｋｓとして選択する（ステップＳ１７１２）。なお、上述したように、さらに、傍受回数を選択基準として用いてもよい。

[0159] これにより、管理サーバ１０１は、少なくとも最大ノード数ではないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択することができる。なお、ステップＳ１７０９のエラー処理の具体例として、たとえば、抽出部１１０２が、携帯端末ＭＴを介して、暗号化パケットＳＰｉを復号するための暗号鍵Ｋｉを抽出できなかった旨のエラーメッセージをノードＮに送信することにしてもよい。

[0160] ステップＳ１７０９のエラー処理は、たとえば、暗号化パケットＳＰｉが改ざんされた場合や暗号化パケットＳＰｉの一部が欠落した場合などに実行される。このエラー処理によれば、ノードＮによる暗号化パケットＳＰｉの再送信を促すことができる。

[0161] また、図１７のステップＳ１７１０では、暗号鍵Ｋｉとノード数とを抽出することとしているが、ステップＳ１７１０ではノード数のみを抽出し、ステップＳ１７１２において、選択鍵Ｋｓが決定されたときに選択鍵Ｋｓのみを抽出することとしてもよい。これにより、選択候補ではあるが最終的に選択されなかった暗号鍵Ｋｉの抽出をおこなう必要がなく、鍵抽出処理（ステップＳ１６０２）の高速化を図ることができる。

[0162] ＜鍵抽出処理（その２）手順＞

つぎに、図１６に示したステップＳ１６０２の鍵抽出処理（その２）の具体的な処理手順について説明する。以下に説明する鍵抽出処理（その２）は、暗号化パケットＳＰｉに含まれるＧＷアドレスが暗号化されている場合（図１２を参照）の処理である。

[0163] 図１８は、ステップＳ１６０２の鍵抽出処理（その２）の具体的な処理手

順の一例を示すフローチャートである。図１８のフローチャートにおいて、まず、管理サーバ１０１は、抽出部１１０２により、ゲートウェイＧｉの「ｉ」を「ｉ＝１」で初期化する（ステップＳ１８０１）。そして、管理サーバ１０１は、抽出部１１０２により、暗号鍵ＤＢ１１０の中のゲートウェイＧｉ固有の暗号鍵Ｋｉを用いて、図１６に示したステップＳ１６０１において受信された暗号化パケットＳＰｉを復号する（ステップＳ１８０２）。

[0164] このあと、管理サーバ１０１は、抽出部１１０２により、暗号化パケットＳＰｉの復号に成功したか否かを判断する（ステップＳ１８０３）。ここで、暗号化パケットＳＰｉの復号に失敗した場合（ステップＳ１８０３：Ｎｏ）、管理サーバ１０１は、抽出部１１０２により、ゲートウェイＧｉの「ｉ」をインクリメントして（ステップＳ１８０４）、「ｉ」が「ｎ」より大きいか否かを判断する（ステップＳ１８０５）。

[0165] ここで、「ｉ」が「ｎ」以下の場合（ステップＳ１８０５：Ｎｏ）、ステップＳ１８０２に戻る。一方、「ｉ」が「ｎ」より大きい場合（ステップＳ１８０５：Ｙｅｓ）、管理サーバ１０１は、別の暗号化パケットＳＰｉ（同一暗号化パケットＳＰｉではない）があるか否かを判断する（ステップＳ１８０６）。

[0166] 別の暗号化パケットＳＰｉがある場合（ステップＳ１８０６：Ｙｅｓ）、ステップＳ１８０１に戻る。一方、別の暗号化パケットＳＰｉがない場合（ステップＳ１８０６：Ｎｏ）、管理サーバ１０１は、ステップＳ１８０９で抽出済みの暗号鍵Ｋｉがあるか否かを判断する（ステップＳ１８０７）。抽出済みの暗号鍵Ｋｉがない場合（ステップＳ１８０７：Ｎｏ）、管理サーバ１０１は、抽出部１１０２により、エラー処理を実行して（ステップＳ１８０８）、管理サーバ１０１の一連の処理を終了する。エラー処理の具体例は、上述したステップＳ１７０９と同様である。

[0167] 一方、抽出済みの暗号鍵Ｋｉがある場合（ステップＳ１８０７：Ｙｅｓ）、管理サーバ１０１は、選択候補の各暗号鍵Ｋｉに関連付けられているノード数により、選択候補の各暗号鍵Ｋｉの中から、新規ノードＮｘに設定させ

る暗号鍵Ｋｉを選択鍵Ｋｓとして選択する（ステップＳ１８１１）。なお、上述したように、さらに、傍受回数を選択基準として用いてもよい。

[0168] 一方、ステップＳ１８０３において、暗号化パケットＳＰｉの復号に成功した場合（ステップＳ１８０３：Ｙｅｓ）、管理サーバ１０１は、抽出部１１０２により、暗号鍵ＤＢ１１０の中から暗号鍵Ｋｉおよび暗号鍵Ｋｉに関連付けられているノード数を抽出する（ステップＳ１８０９）。そして、管理サーバ１０１は、別の暗号化パケットＳＰｉ（同一暗号化パケットＳＰｉではない）があるか否かを判断する（ステップＳ１８１０）。

[0169] 別の暗号化パケットＳＰｉがある場合（ステップＳ１８１０：Ｙｅｓ）、ステップＳ１８０１に戻る。これにより、管理サーバ１０１は、ＧＷアドレスが一致する暗号鍵Ｋｉを選択候補として抽出することができる。

[0170] 一方、別の暗号化パケットＳＰｉがない場合（ステップＳ１８１０：Ｎｏ）、選択候補が抽出済みとなるため、管理サーバ１０１は、選択候補の各暗号鍵Ｋｉに関連付けられているノード数により、選択候補の各暗号鍵Ｋｉの中から、新規ノードＮｘに設定させる暗号鍵Ｋｉを選択鍵Ｋｓとして選択する（ステップＳ１８１１）。なお、上述したように傍受回数を選択基準として用いてもよい。

[0171] これにより、暗号化パケットＳＰｉのヘッダ部１２１０にＧＷアドレスが含まれていない場合であっても、暗号鍵ＤＢ１１０の中から、選択鍵Ｋｓを選択することができる。

[0172] また、図１８のステップＳ１８０９では、暗号鍵Ｋｉとノード数とを抽出することとしているが、ステップＳ１８０９ではノード数のみを抽出し、ステップＳ１８１１において、選択鍵Ｋｓが決定されたときに選択鍵Ｋｓのみを抽出することとしてもよい。これにより、選択候補ではあるが最終的に選択されなかった暗号鍵Ｋｉの抽出をおこなう必要がなく、鍵抽出処理（ステップＳ１６０２）の高速化を図ることができる。

[0173] 以上説明したように、本実施の形態によれば、アドホックネットワークＡｉ内のノードＮは、携帯端末ＭＴを介して、ゲートウェイＧｉからブロード

キャストされた暗号化パケットＳＰｉを管理サーバ１０１に送信することができる。この結果、ノードＮは、携帯端末ＭＴを介して、暗号化パケットＳＰｉを復号するためのゲートウェイＧｉ固有の暗号鍵Ｋｉの中から選択された選択鍵Ｋｓを、管理サーバ１０１から受信して設定することができる。

[0174] このように、ノードＮが、セキュア通信のための暗号鍵Ｋｉが未設定でも受信できるゲートウェイＧｉからの暗号化パケットＳＰｉを手掛かりに、携帯端末ＭＴを介して、管理サーバ１０１に鍵要求することで、選択鍵Ｋｓを取得することができる。これにより、ノードＮの初期導入時などにおいて、作業員ＯＰが地理的に絞り込まれた候補となるゲートウェイとノードＮとの通信状況をしらみつぶしに確認するなどの作業が不要となり、ノードＮに対する暗号鍵Ｋｉの設定作業の効率化を図ることができる。また、確認作業のために候補となる各ゲートウェイの暗号鍵を携帯端末ＭＴなどに記録しておく必要がないため、持ち運びの際の情報漏洩のリスクを低減させることができる。

[0175] また、本実施の形態によれば、ノードＮは、複数のゲートウェイＧｉからブロードキャストされた暗号化パケットＳＰｉを受信（傍受）した場合、ノード数が最大でないアドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉが、設定されることとなる。したがって、複数のアドホックネットワークのうちノード数が少ないアドホックネットワークＡｉのノード数を増加させることができ、複数のアドホックネットワーク間のノード数の平均化を図ることができる。

[0176] このようにノード数の平均化を図ることで、複数のアドホックネットワーク間での通信負荷のばらつきの低減化を図り、また、ゲートウェイに障害が発生したときのリスク分散をおこなうことができる。したがって、複数のアドホックネットワーク全体での通信の安定性の向上を図ることができる。

[0177] さらに、選択鍵Ｋｓの選択基準としてノード数および各暗号化パケットＳＰｉの傍受回数を利用することができる。外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホッ

クネットワーク内のマルチホップ通信の通信経路の多さに比例する。

[0178] したがって、ノード数が少なく（好ましくは最小）、かつ、傍受回数が多い（好ましくは最大の）アドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、ノード数の平均化を図りつつ、新規ノードＮｘは、最も安定性の高いアドホックネットワークＡｉで通信をおこなうことができる。

[0179] 一方、ノード数が少なく（好ましくは最小）、かつ、傍受回数が少ない（好ましくは最小の）アドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘ導入の際、導入先のアドホックネットワークＡｉの通信経路を増強することができる。これにより、ノード数の平均化を図りつつ、通信経路が少ないアドホックネットワークＡｉでの通信の安定性の向上を図ることができる。

[0180] 以上のことから、本実施の形態にかかる鍵設定方法、ノード、サーバおよびネットワークシステムによれば、アドホックネットワーク内のノードに対する暗号鍵の設定作業にかかる作業員の作業負担の軽減化および作業時間の短縮化を図ることができるという効果を奏する。また、複数のアドホックネットワーク間のノードの平均化を図ることにより通信の安定化を図ることができるという効果を奏する。

[0181] なお、上述した実施の形態では、選択基準としてノード数を利用したり、ノード数および各暗号化パケットＳＰｉの傍受回数を利用した例について説明したが、ノード数を利用せずに各暗号化パケットＳＰｉの傍受回数のみを利用することとしてもよい。外乱によって無線通信の状態が変化しやすいアドホックネットワークＡｉでは、傍受回数の多さは、アドホックネットワーク内のマルチホップ通信の通信経路の多さに比例する。

[0182] したがって、傍受回数が多い（好ましくは最大の）アドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘは、最も安定性の高いアドホックネットワークＡｉで通信をおこなうことができる。

[0183] これとは逆に、傍受回数が少ない（好ましくは最小の）アドホックネットワークＡｉのゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとすることで、新規ノードＮｘ導入の際、導入先のアドホックネットワークＡｉの通信経路を増強することができる。これにより、通信経路が少ないアドホックネットワークＡｉでの通信の安定性の向上を図ることができる。

[0184] また、傍受回数のみ利用する場合であっても、傍受回数が同数になった場合には、ノード数の多さを選択基準として利用してもよい。

[0185] なお、本実施の形態で説明した鍵設定方法は、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。本鍵設定プログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。

符号の説明

[0186] １００　ネットワークシステム

１０１　管理サーバ

１１０　暗号鍵ＤＢ

９０１　パケット受信部

９０２　検知部

９０３　パケット送信部

９０４　鍵受信部

９０５　設定部

１１０１　受信部

１１０２　抽出部

１１０３　送信部

１１２１　特定部

１１２２　復号部

１１２３　選択部

Ｋｓ　選択鍵

ＭＴ　携帯端末

Ｎ　ノード

Ｎｘ　新規ノード

請求の範囲

[請求項1] アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークからのパケットを受信可能なノードが実行する鍵設定方法であって、

前記複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを、前記複数のアドホックネットワークから受信するパケット受信工程と、

前記アドホックネットワーク群の各アドホックネットワーク内のゲートウェイ固有の鍵およびノード数を保持するサーバと通信可能な携帯端末との接続を検知する検知工程と、

前記検知工程によって前記携帯端末との接続が検知された場合、前記携帯端末を介して、前記パケット受信工程によって受信された前記複数の暗号化パケットを前記サーバに送信するパケット送信工程と、

前記携帯端末を介して、前記複数のアドホックネットワークの中で前記ノード数が最大ではないいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を前記サーバから受信する鍵受信工程と、

前記鍵受信工程によって受信された鍵を、前記いずれかのアドホックネットワーク内でマルチホップ通信させるパケットを暗号化するための鍵に設定する設定工程と、

を含むことを特徴とする鍵設定方法。

[請求項2] 前記パケット送信工程は、

前記パケット受信工程によって同一暗号化パケットが複数回受信された場合、前記同一暗号化パケットを１回のみ、前記サーバに送信することを特徴とする請求項１に記載の鍵設定方法。

[請求項3] 前記パケット送信工程は、

前記パケット受信工程によって同一暗号化パケットが複数回受信された場合、前記同一暗号化パケットを前記複数回、前記サーバに送信

することを特徴とする請求項１に記載の鍵設定方法。

[請求項4] アドホックネットワーク群の各ゲートウェイと通信可能であり、前記各ゲートウェイのアドレスと、前記各ゲートウェイ固有の鍵と、前記アドホックネットワーク群の各アドホックネットワーク内に存在するノード数と、を記憶するデータベースを有するサーバが、

前記アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを受信したノードから、当該ノードに接続された携帯端末を介して、前記複数の暗号化パケットを受信する受信工程と、

前記受信工程によって受信された前記複数の暗号化パケットの各暗号化パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定する特定工程と、

前記複数のアドホックネットワークのうち、前記特定工程によって特定されたノード数のうち最大でないいずれかのノード数であるいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を、前記データベースにおいて前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する選択工程と、

前記選択工程によって選択された選択鍵を、前記携帯端末を介して、前記ノードに送信する送信工程と、

を含むことを特徴とする鍵設定方法。

[請求項5] 前記各暗号化パケットを前記データベース内の鍵を用いて復号する復号工程を含み、

前記特定工程は、

前記復号工程によって復号された各パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定することを特徴とす

る請求項４に記載の鍵設定方法。

[請求項6] 前記選択工程は、

前記ノード数が最小であるアドホックネットワーク内のゲートウェイ固有の鍵を、前記データベースにおいて前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択することを特徴とする請求項５に記載の鍵設定方法。

[請求項7] 前記選択工程は、

前記各暗号化パケットの受信回数に基づいて、前記データベースにおいて前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する請求項５に記載の鍵設定方法。

[請求項8] アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークからのパケットを受信可能なノードであって、

前記複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを、前記複数のアドホックネットワークから受信するパケット受信手段と、

前記アドホックネットワーク群の各アドホックネットワーク内のゲートウェイ固有の鍵およびノード数を保持するサーバと通信可能な携帯端末との接続を検知する検知手段と、

前記検知手段によって前記携帯端末との接続が検知された場合、前記携帯端末を介して、前記パケット受信手段によって受信された前記複数の暗号化パケットを前記サーバに送信するパケット送信手段と、

前記携帯端末を介して、前記複数のアドホックネットワークの中で前記ノード数が最大ではないいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を前記サーバから受信する鍵受信手段と、

前記鍵受信手段によって受信された鍵を、前記いずれかのアドホックネットワーク内でマルチホップ通信させるパケットを暗号化するための鍵に設定する設定手段と、

を備えることを特徴とするノード。

[請求項9] 前記パケット送信手段は、

前記パケット受信手段によって同一暗号化パケットが複数回受信された場合、前記同一暗号化パケットを１回のみ、前記サーバに送信することを特徴とする請求項８に記載のノード。

[請求項10] 前記パケット送信手段は、

前記パケット受信手段によって同一暗号化パケットが複数回受信された場合、前記同一暗号化パケットを前記複数回、前記サーバに送信することを特徴とする請求項８に記載のノード。

[請求項11] アドホックネットワーク群の各ゲートウェイと通信可能なサーバであって、

前記各ゲートウェイのアドレスと、前記各ゲートウェイ固有の鍵と、前記アドホックネットワーク群の各アドホックネットワーク内に存在するノード数と、を記憶する記憶手段と、

前記アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを受信したノードから、当該ノードに接続された携帯端末を介して、前記複数の暗号化パケットを受信する受信手段と、

前記受信手段によって受信された前記複数の暗号化パケットの各暗号化パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定する特定手段と、

前記複数のアドホックネットワークのうち、前記特定手段によって特定されたノード数のうち最大でないいずれかのノード数であるいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を、前記記憶手段において前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する選択手段と、

前記選択手段によって選択された選択鍵を、前記携帯端末を介して、前記ノードに送信する送信手段と、

を備えることを特徴とするサーバ。

[請求項12] 前記各暗号化パケットを前記データベース内の鍵を用いて復号する復号手段を備え、

前記特定手段は、

前記復号手段によって復号された各パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定することを特徴とする請求項１１に記載のサーバ。

[請求項13] 前記選択手段は、

前記ノード数が最小であるアドホックネットワーク内のゲートウェイ固有の鍵を、前記記憶手段において前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択することを特徴とする請求項１１に記載のサーバ。

[請求項14] 前記選択手段は、

前記各暗号化パケットの受信回数に基づいて、前記データベースにおいて前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する請求項１１に記載のサーバ。

[請求項15] アドホックネットワーク群のうち通信圏内にある複数のアドホックネットワークからのパケットを受信可能なノードと、前記アドホックネットワーク群の各ゲートウェイと通信可能なサーバと、を備えるネットワークシステムであって、

前記サーバは、

前記アドホックネットワーク群の各ゲートウェイのアドレスと、前記各ゲートウェイ固有の鍵と、前記アドホックネットワーク群の各アドホックネットワーク内に存在するノード数と、を記憶する記憶手段と、

前記複数のアドホックネットワークの各ゲートウェイから同時通報された当該各ゲートウェイ固有の鍵を用いて暗号化された複数の暗号化パケットを、前記ノードに接続された携帯端末を介して、前記ノードから受信する受信手段と、

前記受信手段によって受信された前記複数の暗号化パケットの各暗号化パケットに含まれている各ゲートウェイのアドレスに基づいて、前記各ゲートウェイが所属するアドホックネットワーク内に存在するノード数を特定する特定手段と、

前記複数のアドホックネットワークのうち、前記特定手段によって特定されたノード数のうち最大でないいずれかのノード数であるいずれかのアドホックネットワーク内のゲートウェイ固有の鍵を、前記記憶手段において前記複数のアドホックネットワーク内の各ゲートウェイ固有の鍵の中から選択する選択手段と、

前記選択手段によって選択された選択鍵を、前記携帯端末を介して、前記ノードに送信する送信手段と、を備え、

前記ノードは、

前記複数の暗号化パケットを前記複数のアドホックネットワークから受信するパケット受信手段と、

前記サーバと通信可能な前記携帯端末との接続を検知する検知手段と、

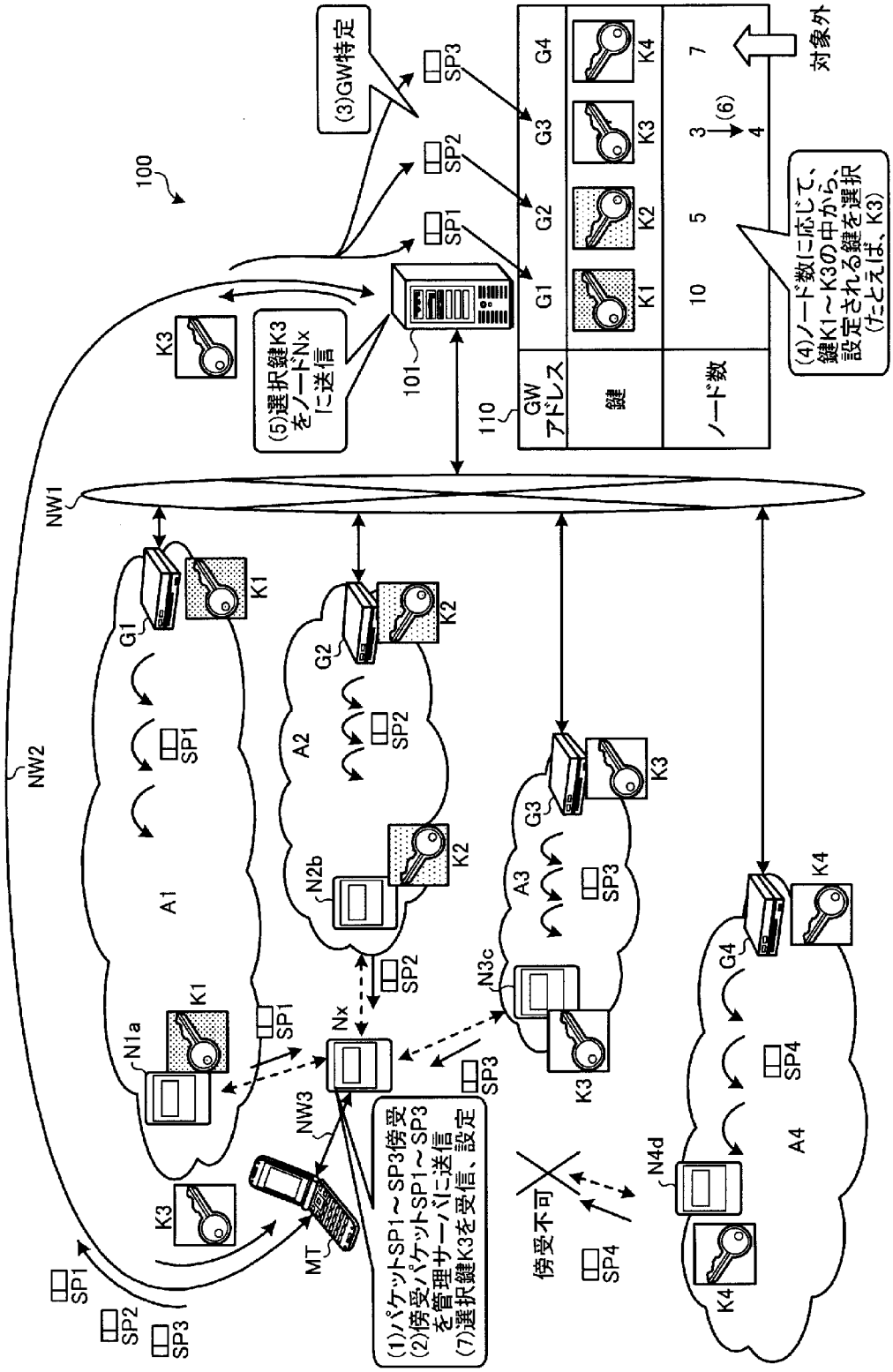
前記検知手段によって前記携帯端末との接続が検知された場合、前記携帯端末を介して、前記パケット受信手段によって受信された前記複数の暗号化パケットを前記サーバに送信するパケット送信手段と、

前記送信手段によって送信された前記選択鍵を、前記携帯端末を介して、前記サーバから受信する鍵受信手段と、

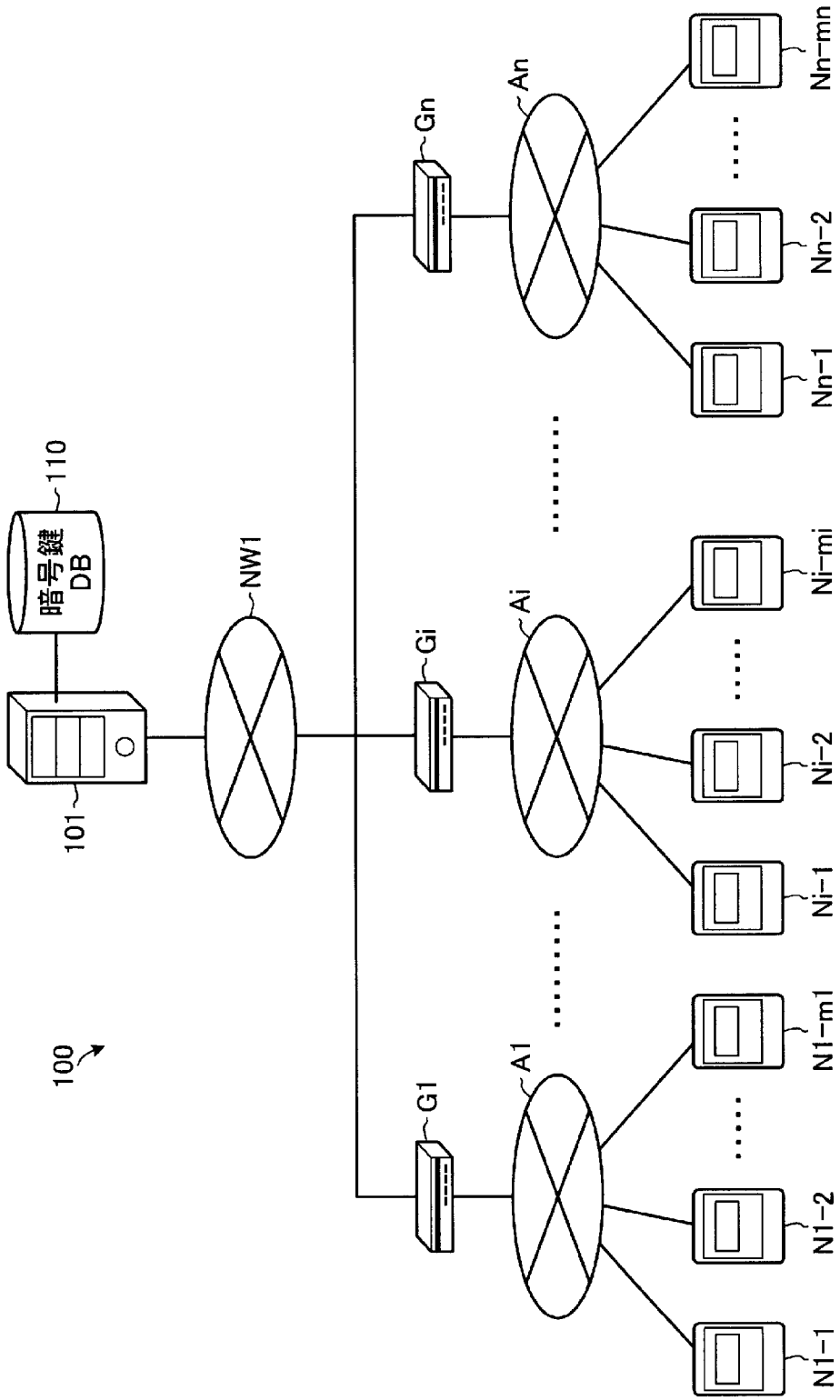
前記鍵受信手段によって受信された前記選択鍵を、前記いずれかのアドホックネットワーク内でマルチホップ通信させるパケットを暗号化するための鍵に設定する設定手段と、

を備えることを特徴とするネットワークシステム。

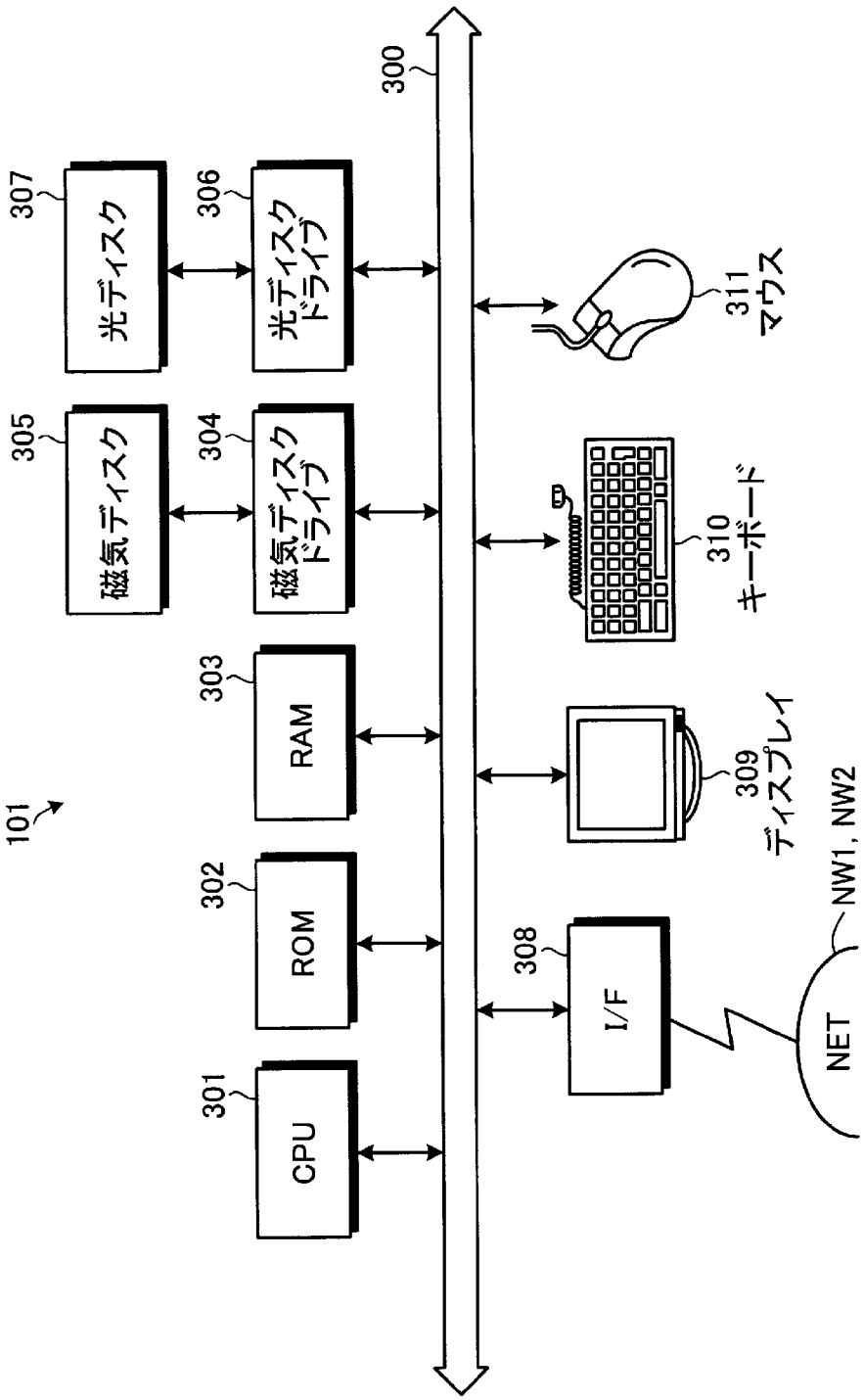
[図1]


100
101
110
GW アドレス
鍵
ノード数
G1
G2
G3
G4
K1
K2
K3
K4
10
5
3
4
7
(6)
対象外
(3)GW特定
(4)ノード数に応じて、鍵K1～K3の中から、設定される鍵を選択(たとえば、K3)
(5)選択鍵K3をノードNxに送信
(1)パケットSP1～SP3傍受
(2)傍受パケットSP1～SP3を管理サーバに送信
(7)選択鍵K3を受信、設定
傍受不可
NW1
NW2
NW3
A1
A2
A3
A4
N1a
N2b
N3c
N4d
Nx
MT
SP1
SP2
SP3
SP4

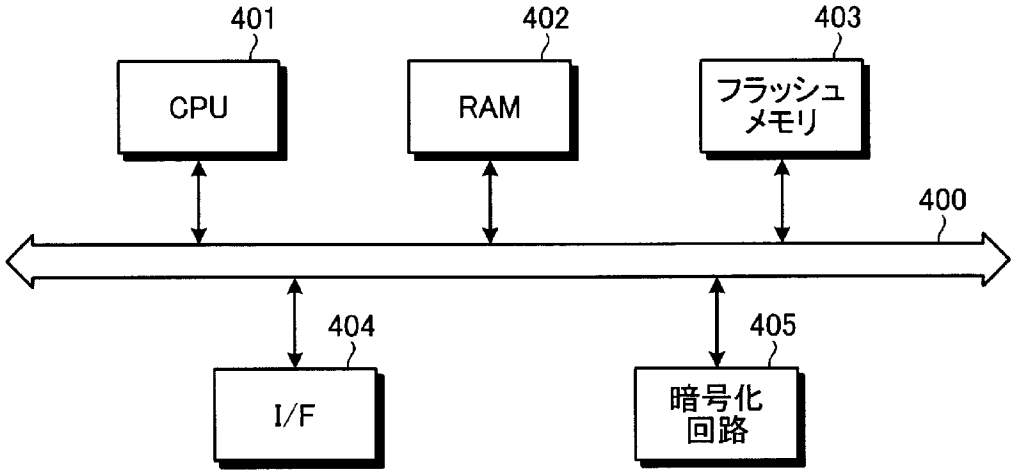
[図2]


100
101
110
暗号鍵
DB
NW1
G1
Gi
Gn
A1
Ai
An
N1-1
N1-2
N1-m1
Ni-1
Ni-2
Ni-mi
Nn-1
Nn-2
Nn-mn

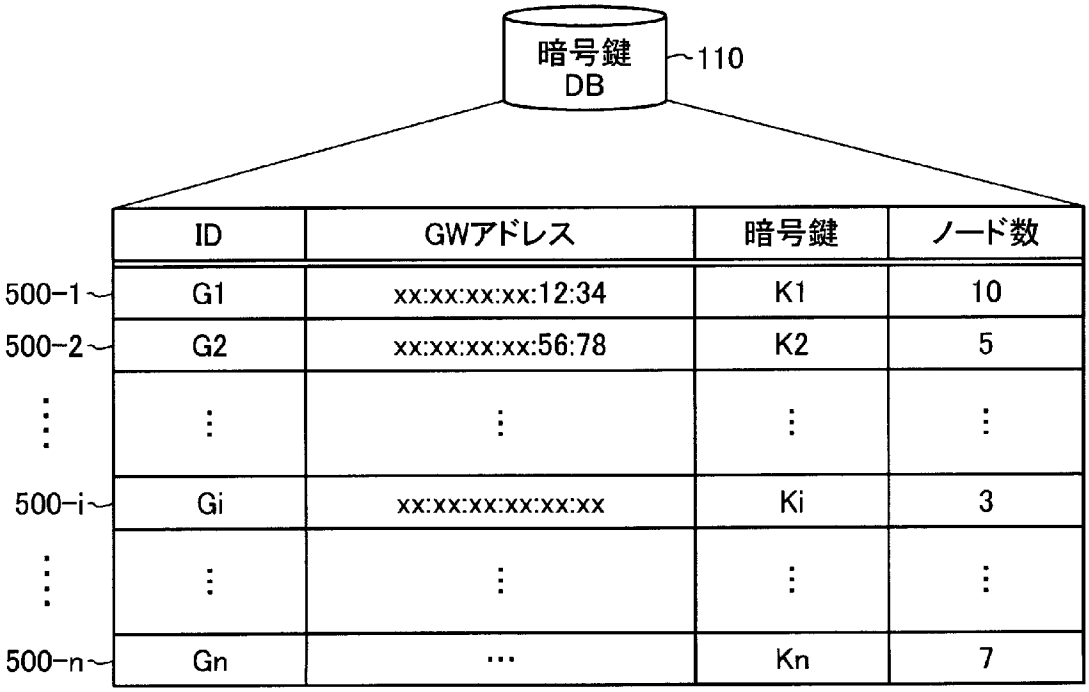
[図3]


101
300
301
CPU
302
ROM
303
RAM
304
磁気ディスクドライブ
305
磁気ディスク
306
光ディスクドライブ
307
光ディスク
308
I/F
309
ディスプレイ
310
キーボード
311
マウス
NET
NW1, NW2

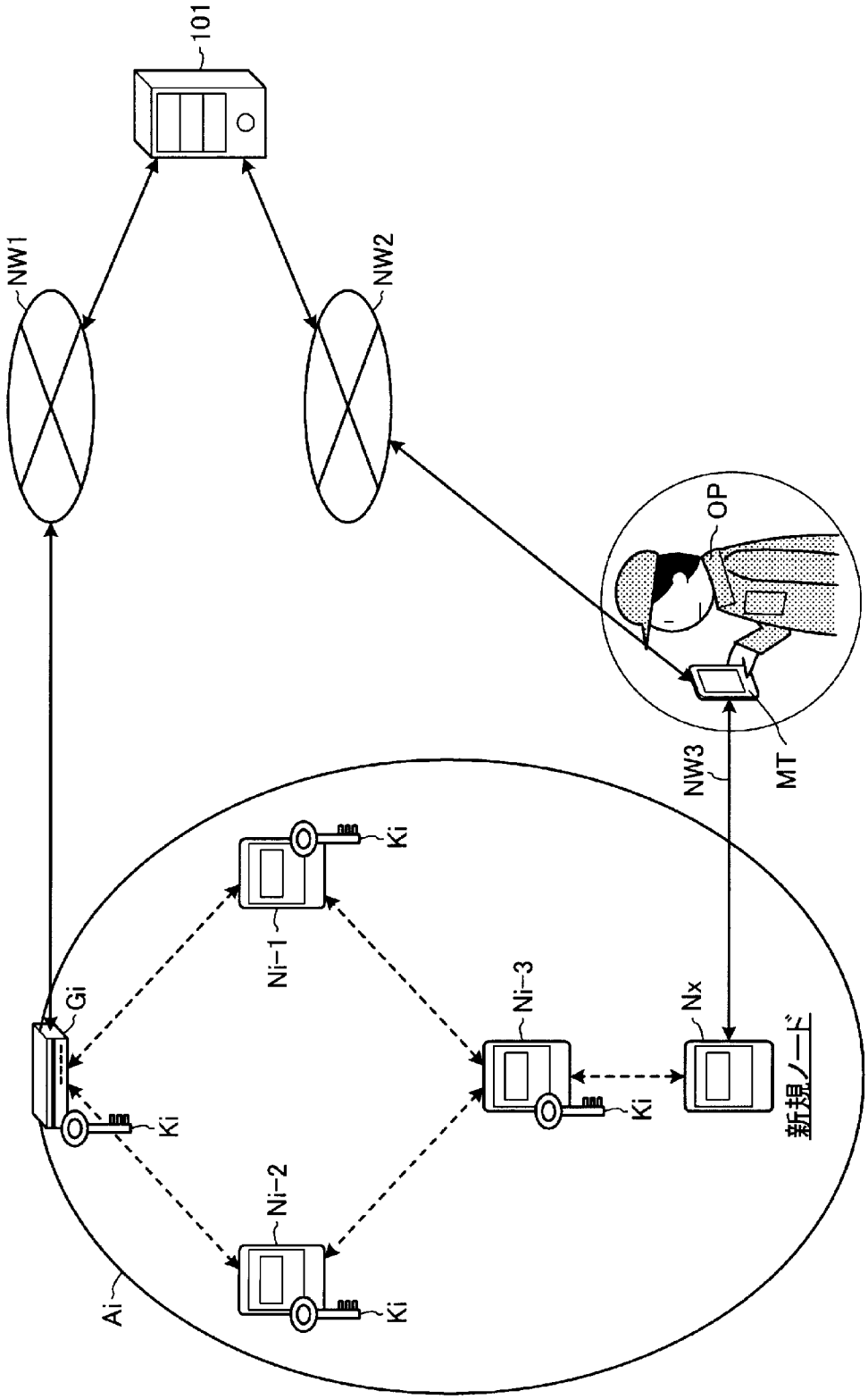
[図4]


401
CPU
402
RAM
403
フラッシュ
メモリ
400
404
I/F
405
暗号化
回路

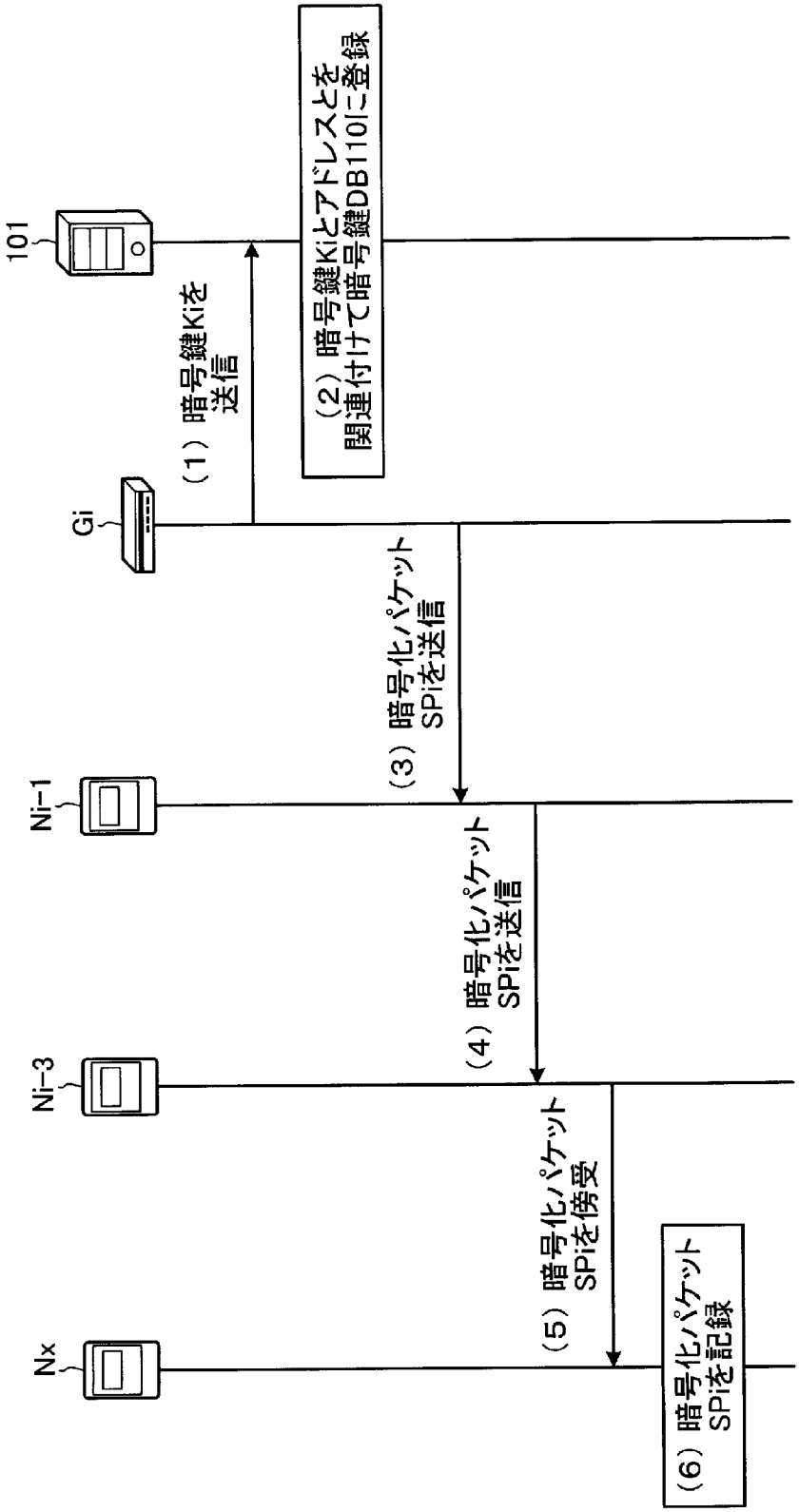
[図5]


暗号鍵
DB
110
ID
GWアドレス
暗号鍵
ノード数
500-1
G1
xx:xx:xx:xx:12:34
K1
10
500-2
G2
xx:xx:xx:xx:56:78
K2
5
500-i
Gi
xx:xx:xx:xx:xx:xx
Ki
3
500-n
Gn
…
Kn
7

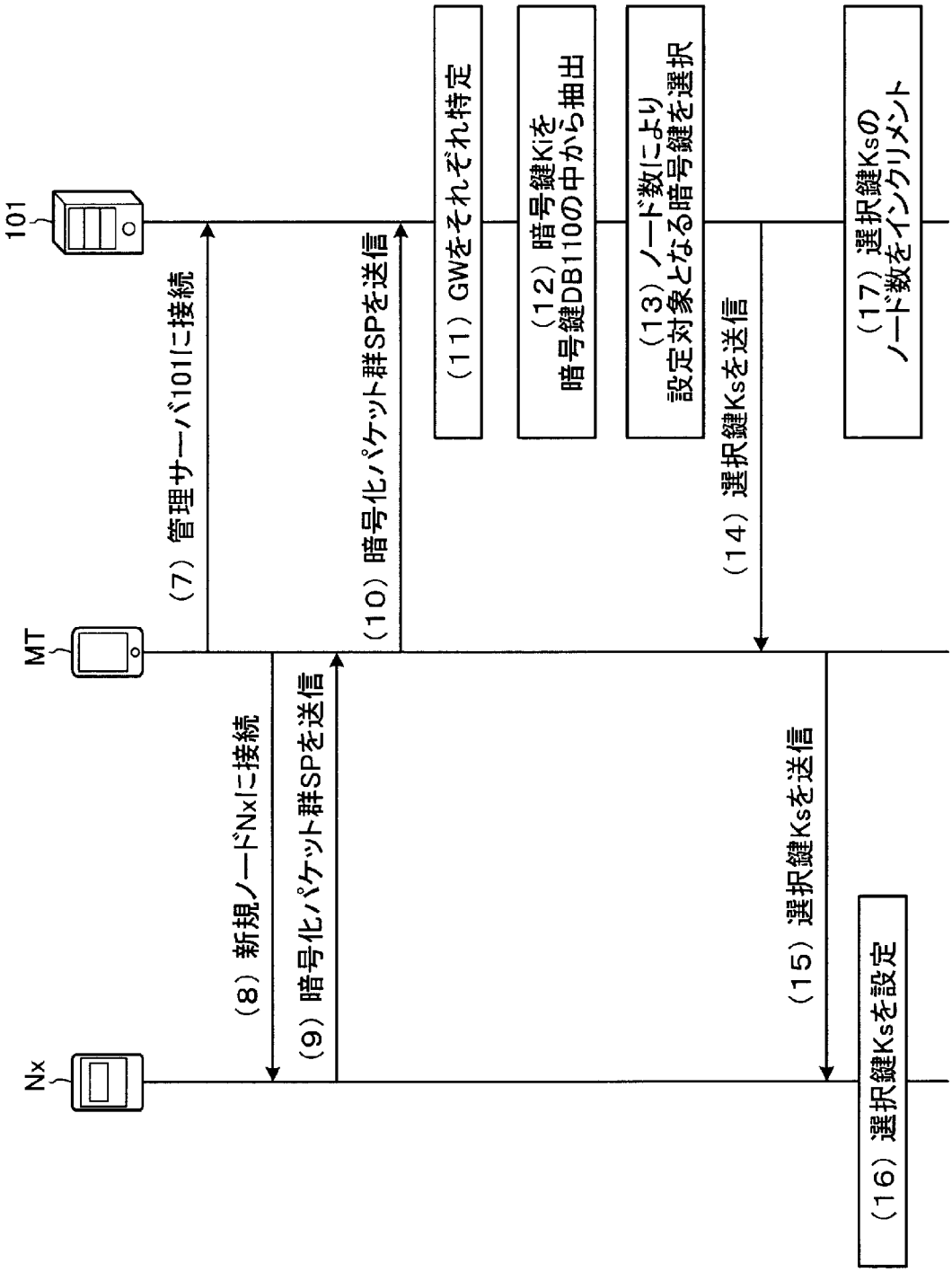
[図6]



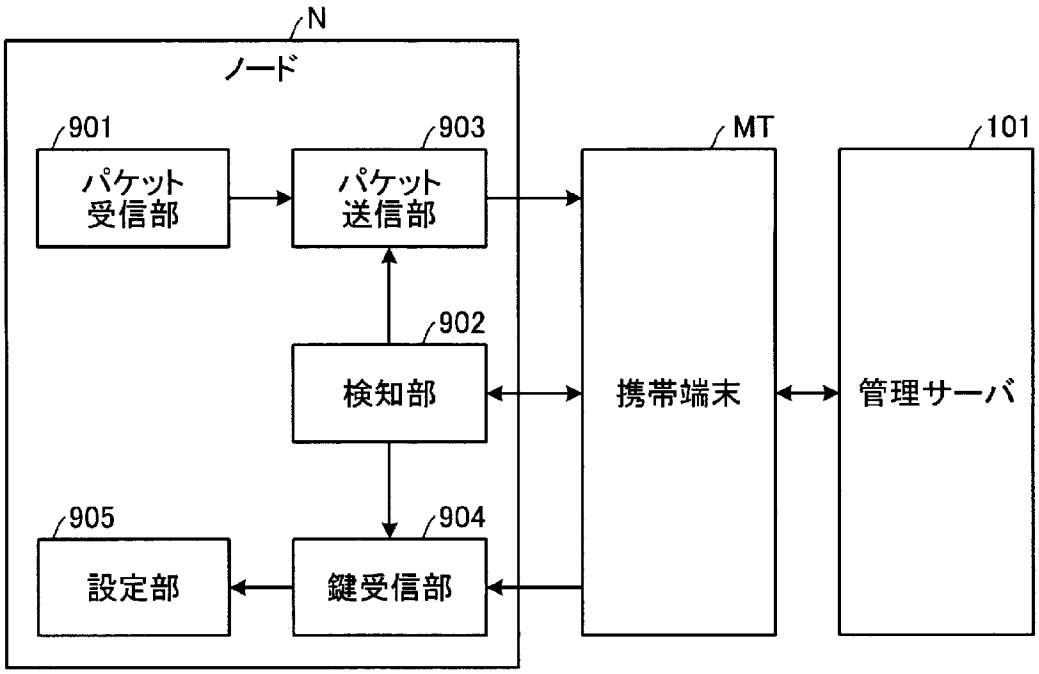
[図7]


101
Gi
Ni−1
Ni−3
Nx
（1）暗号鍵Kiを送信
（2）暗号鍵Kiとアドレスとを関連付けて暗号鍵DB110に登録
（3）暗号化パケットSPiを送信
（4）暗号化パケットSPiを送信
（5）暗号化パケットSPiを傍受
（6）暗号化パケットSPiを記録

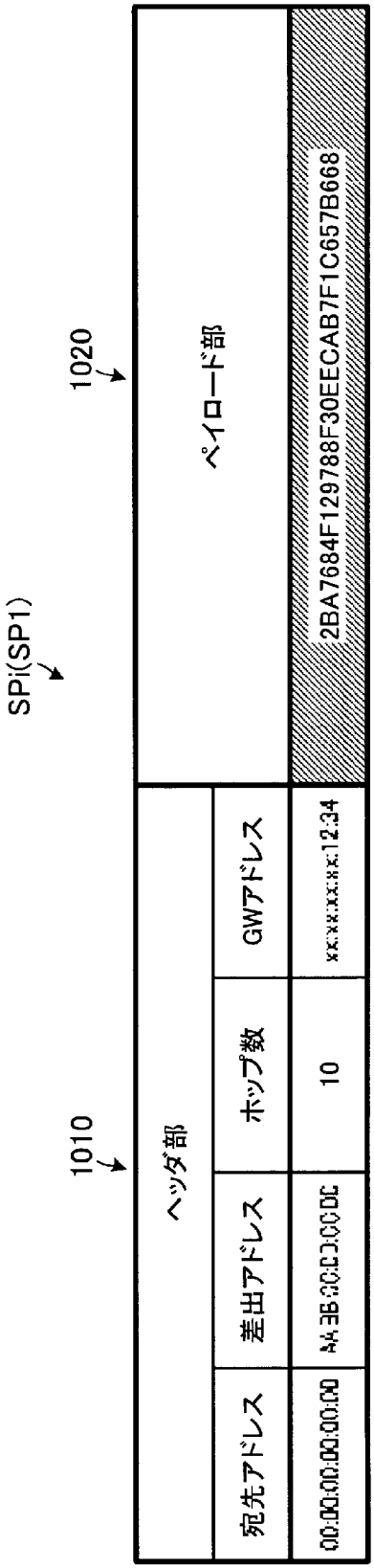
[図8]


101
MT
Nx
(7) 管理サーバ101に接続
(8) 新規ノードNxに接続
(9) 暗号化パケット群SPを送信
(10) 暗号化パケット群SPを送信
(11) GWをそれぞれ特定
(12) 暗号鍵Kiを
暗号鍵DB110の中から抽出
(13) ノード数により
設定対象となる暗号鍵を選択
(14) 選択鍵Ksを送信
(15) 選択鍵Ksを送信
(16) 選択鍵Ksを設定
(17) 選択鍵Ksの
ノード数をインクリメント

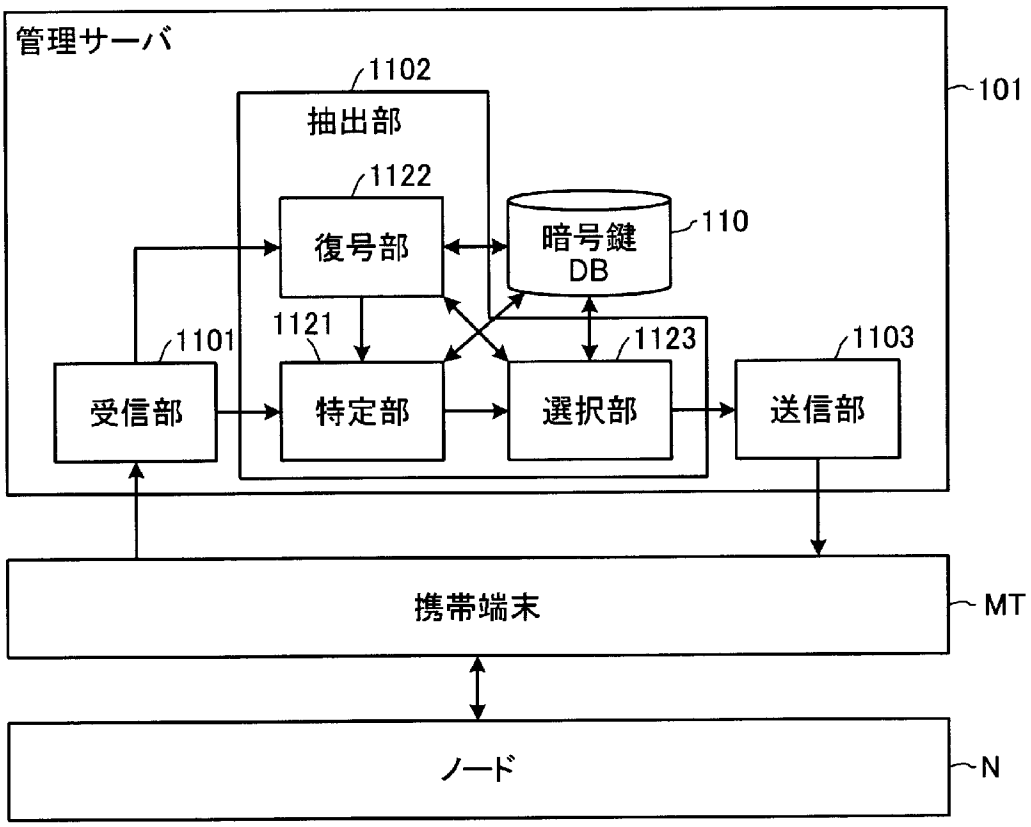
[図9]


N
ノード
901
パケット
受信部
903
パケット
送信部
902
検知部
905
設定部
904
鍵受信部
MT
携帯端末
101
管理サーバ

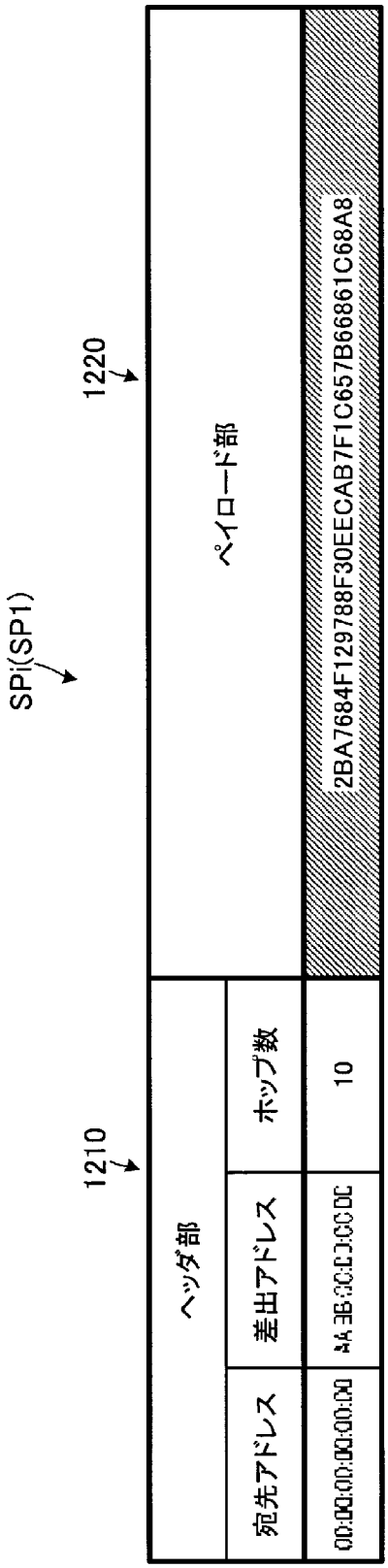
[図10]


SPi(SP1)
1010
1020
ヘッダ部
宛先アドレス
差出アドレス
ホップ数
GWアドレス
00:00:00:00:00:00
AA:BB:CC:DD:EE:FF
10
xx:xx:xx:xx:12:34
ペイロード部
2BA7684F129788F30EECAB7F1C657B668

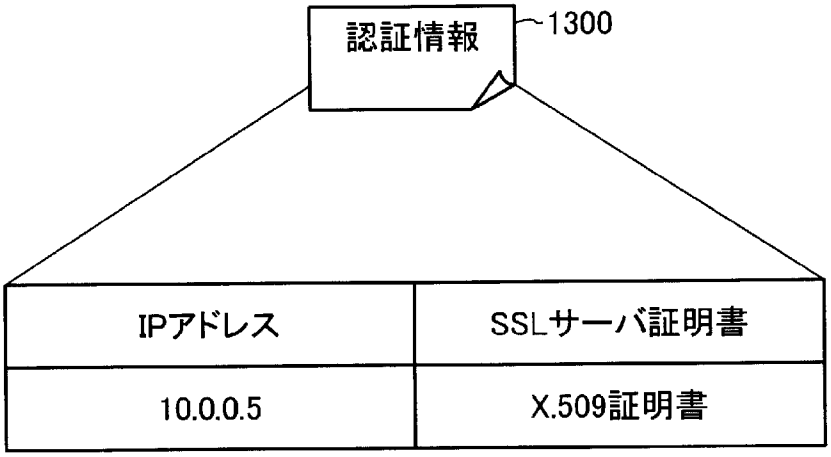
[図11]


管理サーバ
101
1102
抽出部
1122
復号部
暗号鍵
DB
110
1121
1101
1123
1103
受信部
特定部
選択部
送信部
携帯端末
MT
ノード
N

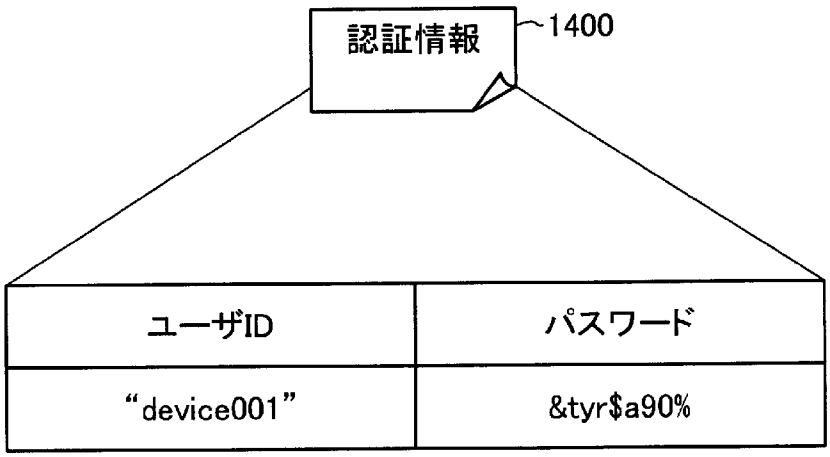
[図12]


SPi(SP1)
1210
1220
ヘッダ部
宛先アドレス
差出アドレス
ホップ数
00:00:00:00:00:00
AA:BB:CC:DD:EE:FF
10
ペイロード部
2BA7684F129788F30EECAB7F1C657B66861C68A8

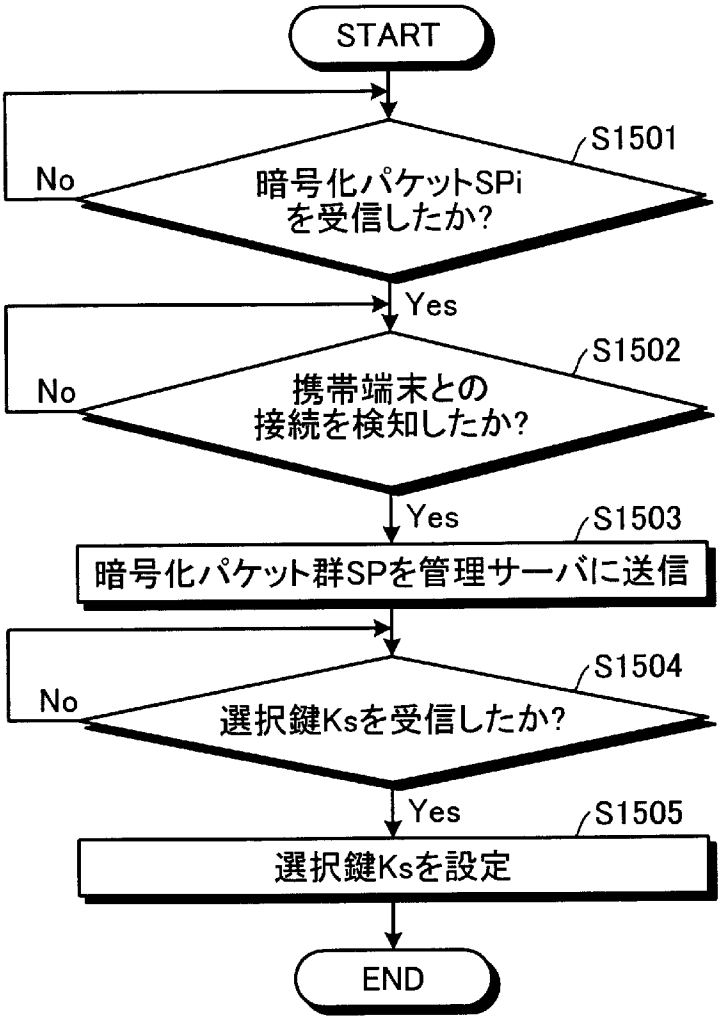
[図13]


認証情報
1300
IPアドレス
SSLサーバ証明書
10.0.0.5
X.509証明書

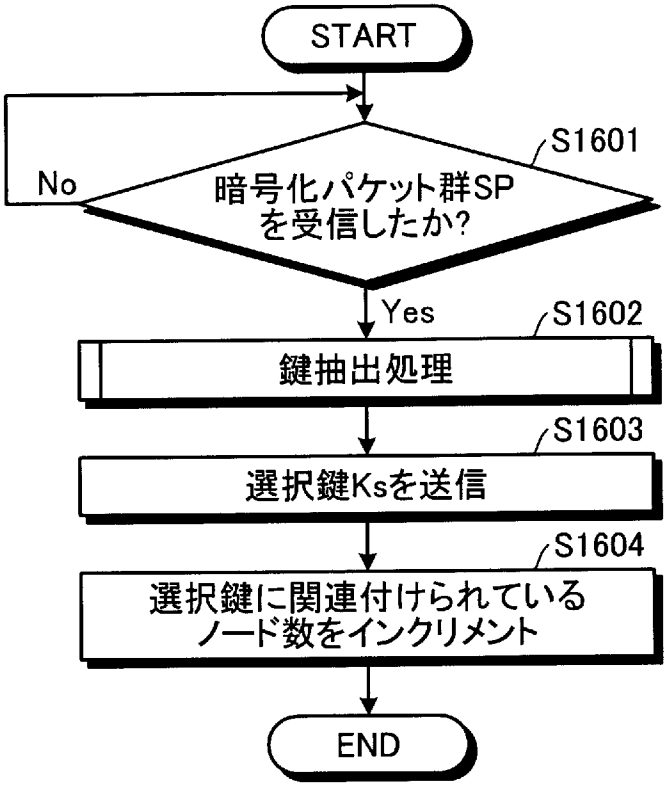
[図14]


認証情報
1400
ユーザID
パスワード
“device001”
&tyr$a90%

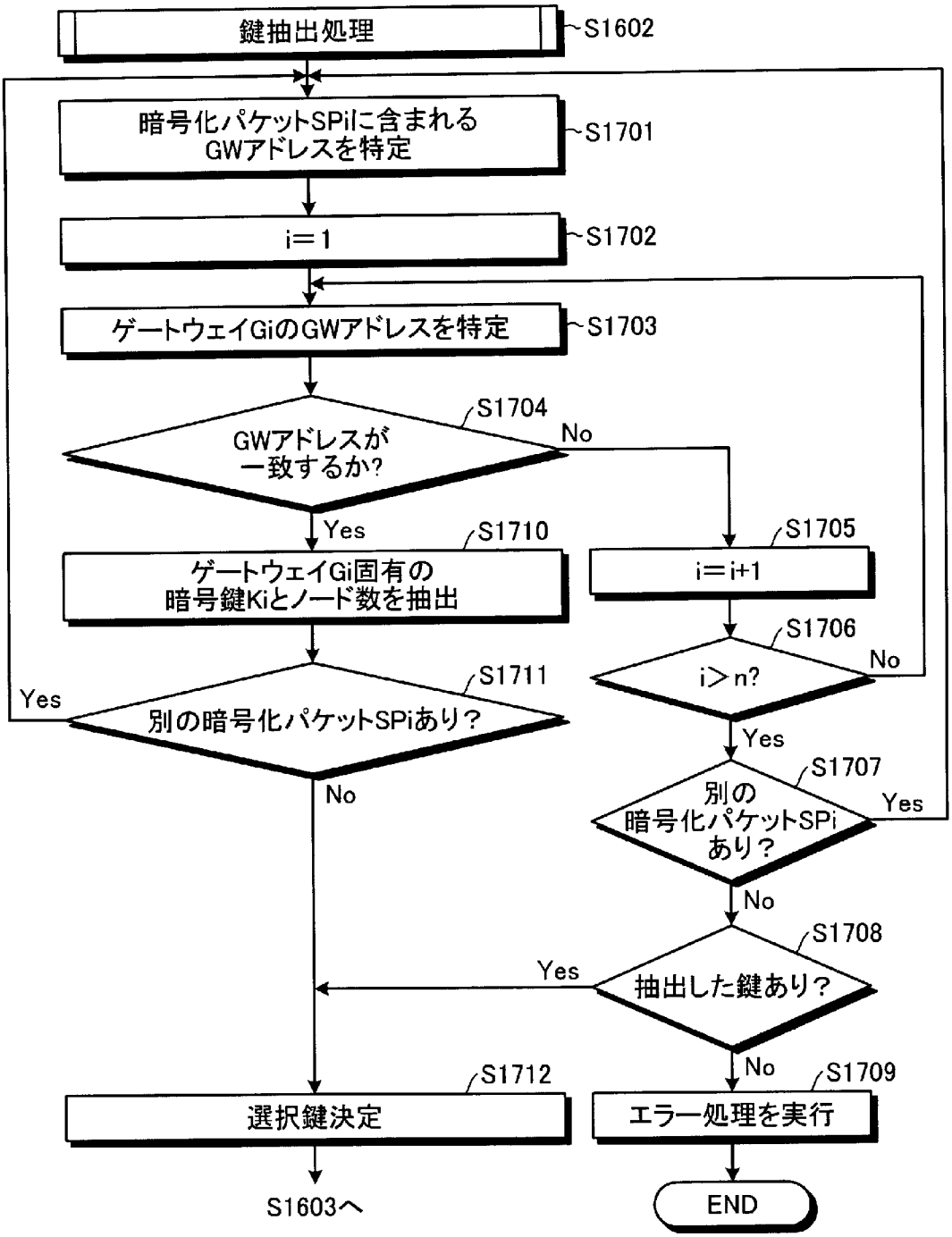
[図15]


START
S1501
暗号化パケットSPi
を受信したか?
No
Yes
S1502
携帯端末との
接続を検知したか?
No
Yes
S1503
暗号化パケット群SPを管理サーバに送信
S1504
選択鍵Ksを受信したか?
No
Yes
S1505
選択鍵Ksを設定
END

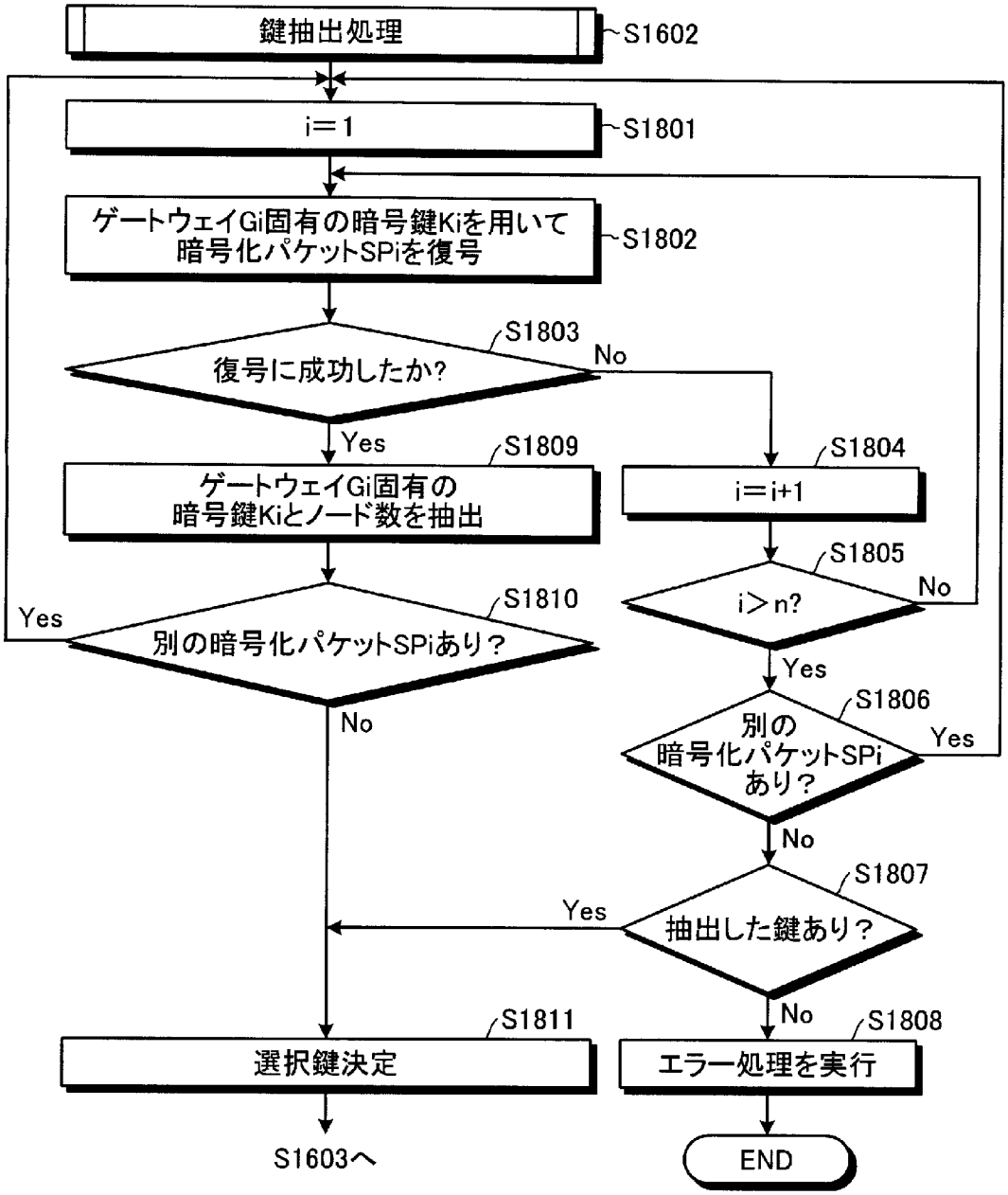
[図16]


START
S1601
暗号化パケット群SP
を受信したか?
No
Yes
S1602
鍵抽出処理
S1603
選択鍵Ksを送信
S1604
選択鍵に関連付けられている
ノード数をインクリメント
END

[図17]


鍵抽出処理
S1602
暗号化パケットSPiに含まれる
GWアドレスを特定
S1701
i=1
S1702
ゲートウェイGiのGWアドレスを特定
S1703
S1704
GWアドレスが
一致するか?
No
Yes
S1710
ゲートウェイGi固有の
暗号鍵Kiとノード数を抽出
S1705
i=i+1
S1706
i>n?
No
Yes
S1711
別の暗号化パケットSPiあり?
Yes
No
S1707
別の
暗号化パケットSPi
あり?
Yes
No
S1708
抽出した鍵あり?
Yes
No
S1712
選択鍵決定
S1709
エラー処理を実行
S1603へ
END

[図18]


鍵抽出処理
S1602
i=1
S1801
ゲートウェイGi固有の暗号鍵Kiを用いて
暗号化パケットSPiを復号
S1802
S1803
復号に成功したか?
No
Yes
S1809
ゲートウェイGi固有の
暗号鍵Kiとノード数を抽出
S1804
i=i+1
S1805
i>n?
No
Yes
S1810
別の暗号化パケットSPiあり?
Yes
No
S1806
別の
暗号化パケットSPi
あり?
Yes
No
S1807
抽出した鍵あり?
Yes
No
S1811
選択鍵決定
S1808
エラー処理を実行
S1603へ
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/051964

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04W84/12*(2009.01)i, *H04W84/18*(2009.01)i, *H04W88/08*(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, H04W84/12, H04W84/18, H04W88/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-67745 A (Fujitsu Ltd.), 15 March 2007 (15.03.2007), entire text; all drawings & US 2007/0047480 A1	1-15
A	JP 2009-535921 A (Motorola, Inc.), 01 October 2009 (01.10.2009), entire text; all drawings & US 2007/0253376 A1 & EP 2022282 A & WO 2007/127637 A2 & CA 2650050 A & RU 2008146960 A	1-15
A	JP 2007-74393 A (NTT Docomo Inc.), 22 March 2007 (22.03.2007), entire text; all drawings (Family: none)	1-15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 25 February, 2011 (25.02.11)	Date of mailing of the international search report 08 March, 2011 (08.03.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/051964

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-116319 A (Saxa, Inc.), 10 May 2007 (10.05.2007), entire text; all drawings (Family: none)	1-15
A	JP 2009-71707 A (Oki Electric Industry Co., Ltd.), 02 April 2009 (02.04.2009), entire text; all drawings (Family: none)	1-15

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０５１９６４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, H04W84/12(2009.01)i, H04W84/18(2009.01)i, H04W88/08(2009.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, H04W84/12, H04W84/18, H04W88/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2007-67745 A (富士通株式会社) 2007.03.15, 全文、全図 & US 2007/0047480 A1	1-15
A	JP 2009-535921 A (モトローラ・インコーポレイテッド) 2009.10.01, 全文、全図 & US 2007/0253376 A1 & EP 2022282 A & WO 2007/127637 A2 & CA 2650050 A & RU 2008146960 A	1-15

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２５．０２．２０１１	国際調査報告の発送日 ０８．０３．２０１１
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　４５３８ 金沢　史明 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2007-74393 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.03.22, 全文、全図 (ファミリーなし)	1-15
A	JP 2007-116319 A (サクサ株式会社) 2007.05.10, 全文、全図 (ファミリーなし)	1-15
A	JP 2009-71707 A (沖電気工業株式会社) 2009.04.02, 全文、全図 (ファミリーなし)	1-15