(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 2012/104976 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/JP2011/051963

(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.

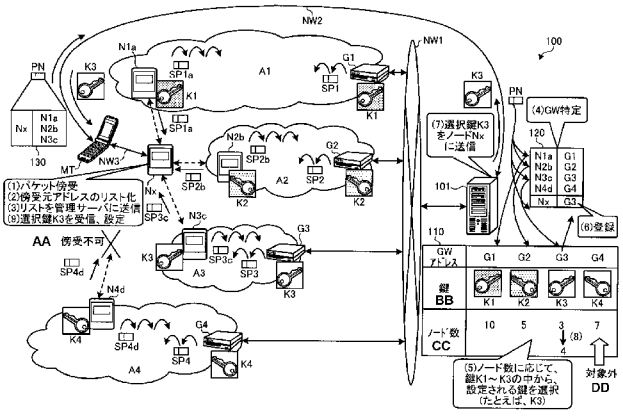
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,

[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 packet.
(2) List intercept source addresses.
(3) Send list to management server.
(4) Specify gateway.
(5) Select key to be set (e.g., K3), from keys (K1-K3) according to the number of nodes.
(6) Register.
(7) Send selected key (K3) to node (Nx).
(9) Receive and set selected key (K3).
110 Gateway address
AA Intercept not possible.
BB Key
CC Number of nodes
DD Not included.

(57) **Abstract**: A new node (Nx) intercepts encrypted packets (SP1a, SP2b, SP3c), extracts addresses for intercept source nodes (N1a, N2b, N3c), and sends a packet (PN) to a management server (101) via a mobile terminal (MT). The management server (101) extracts the addresses for the intercept source nodes (N1a, N2b, N3c) contained in the packet (PN) from the new node (Nx). The management server (101) specifies gateway addresses associated with the addresses for the intercept source nodes (N1a, N2b, N3c) from a node database (120), selects an encryption key (K3) to be set to the new node (Nx) from among encryption keys (K1-K3) associated with the specified gateways (G1-G3), and sends same to the new node (Nx) via the mobile terminal (MT). The new node (Nx) sets the selected key (K3) as the key to encrypt the packet or decode the encrypted packet.

(57) 要約: 新規ノード（Ｎｘ）は、暗号化パケット（ＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ）を傍受し、傍受元ノード（Ｎ１ａ，Ｎ２ｂ，Ｎ３ｃ）のアドレスを抽出し、パケット（ＰＮ）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）からのパケット（ＰＮ）に含まれている傍受元ノード（Ｎ１ａ，Ｎ２ｂ，Ｎ３ｃ）のアドレスを抽出する。管理サーバ（１０１）は、傍受元のノード（Ｎ１ａ，Ｎ２ｂ，Ｎ３ｃ）のアドレスに関連付けされているゲートウェイのアドレスをノードＤＢ（１２０）から特定し、特定されたゲートウェイ（Ｇ１～Ｇ３）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（Ｋ３）を選択し、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、パケットを暗号化、または、暗号化パケットを復号する鍵に設定する。

WO 2012/104976 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、本発明の一観点によれば、複数のアドホックネットワークのうち通信圏内にあるアドホックネットワーク群からのパケットを受信可能なノードが、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前記ノードの通信圏内にある各近隣ノード

から、前記各アドホックネットワーク内のゲートウェイ固有の鍵を用いて暗号化された暗号化パケットを受信し、前記各近隣ノードから受信された暗号化パケット群の各々の暗号化パケットの中から前記各近隣ノードのアドレスを抽出し、前記複数のアドホックネットワーク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、ノード数および前記各アドホックネットワーク内の各ノードのアドレス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、抽出された前記各近隣ノードのアドレスを含むパケットを前記サーバに送信し、送信されたパケットから得られる前記各近隣ノードのアドレスから特定された前記各ゲートウェイが属する前記アドホックネットワーク群のうち、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、前記携帯端末を介して、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が提供される。

[0015] また、本発明の一観点によれば、複数のアドホックネットワークで構成されるネットワークシステムの中の各アドホックネットワーク内のゲートウェイごとにゲートウェイ固有の鍵および配下のノード数を関連付けた第１のデータベースと、前記複数のアドホックネットワーク内のノードごとに所属ゲートウェイの識別情報を関連付けた第２のデータベースと、を有し、前記各アドホックネットワークの各ゲートウェイと通信可能なサーバが、前記複数のアドホックネットワークのいずれのアドホックネットワーク内のゲートウェイ固有の鍵も未設定なノードに接続された携帯端末を介して、前記ノードから前記ノードのアドレスおよび前記ノードの近隣ノードのアドレスを含むパケットを受信し、受信されたパケットに含まれている前記各近隣ノードのアドレスに基づいて、前記各近隣ノードの所属ゲートウェイを、前記第２のデータベースから特定し、特定された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、前記第１のデータベースから特

定し、前記複数のアドホックネットワークのうち、特定された前記各ゲートウェイの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、前記第１のデータベースにおける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が提供される。

発明の効果

[0016] 本発明の一観点による鍵設定方法、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１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１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１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１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、図１に示したノードＤＢの記憶内容の一例を示す説明図である。

[図7]図７は、実施の形態１にかかる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8]図８は、実施の形態１にかかる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9]図９は、実施の形態１にかかる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10]図１０は、ノードの機能的構成例を示すブロック図である。

[図11]図１１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12]図１２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13]図１３は、ノードＤＢの更新の具体例を示す説明図である。

[図14]図１４は、管理サーバの認証情報の一例を示す説明図である。

[図15]図１５は、携帯端末の認証情報の一例を示す説明図である。

[図16]図１６は、実施の形態１にかかる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17]図１７は、実施の形態１にかかる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18]図１８は、実施の形態２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19]図１９は、実施の形態２にかかる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20]図２０は、実施の形態２にかかる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。

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] ＜実施の形態１＞

（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１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１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] ここで、アドホックネットワークＡ１～Ａ４内のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ４ｄを例に挙げて説明する。ノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ４ｄは、それぞれ保持する暗号鍵Ｋ１～Ｋ４で暗号化した暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ４ｄを自律的に送信する。ノードＮ１ａ

，Ｎ２ｂ，Ｎ３ｃ，Ｎ４ｄは、それぞれ暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ４ｄの送信元または同一アドホックネットワーク内の近隣ノードに対する転送元である。

[0024] ノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ４ｄは、それぞれ保持するルーティングテーブルに従って暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ４ｄを送信する。ルーティングテーブルがない場合は、通信圏内のすべての近隣ノードに送信することとなる。いずれにしても近隣ノードには暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ４ｄが送信される。

[0025] 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。したがって、暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃも受信可能である。

[0026] 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。

[0027] 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から送信された暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ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ＳＰ４ｄは傍受されない。

[0028] 新規ノードＮｘは、傍受した暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３

ｃに含まれている傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃのアドレスを抽出し、アドレスリスト１３０を生成する。傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃのアドレスは、暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃの暗号化されていないヘッダ部に記述されているため抽出可能である。新規ノードＮｘは、アドレスリスト１３０を含むパケットＰＮ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ことができる。

[0029] ただし、新規ノードＮｘは、暗号鍵Ｋ１～Ｋ３を保持してないためパケットＰＮを暗号化できない。したがって、新規ノードＮｘが、パケットＰＮを傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ経由で送っても、パケットＰＮは、暗号鍵Ｋ１～Ｋ３で暗号化されていないため、ノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃで破棄されて、管理サーバ１０１に届かない。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、パケットＰＮを管理サーバ１０１に送信する。

[0030] 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。

[0031] 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ＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃを傍受する。暗号化パケットＳＰ４ｄは通信圏外であるため、傍受できない。

[0032] （２）新規ノードＮｘは、傍受した暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃから傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃのアドレスを抽出し、アドレスリスト１３０を生成する。

[0033] （３）新規ノードＮｘは、上記（２）で生成されたアドレスリスト１３０を含むパケットＰＮを携帯端末ＭＴ経由で管理サーバ１０１に送信する。なお

、パケットＰＮには、新規ノードＮｘのアドレスも含ませる。

[0034] （４）管理サーバ１０１は、新規ノードＮｘからパケットＰＮを受信すると、パケットＰＮを解析して、パケットＰＮに含まれている傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃのアドレスと新規ノードＮｘのアドレスを抽出する。そして、管理サーバ１０１は、抽出された傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃのアドレスに関連付けされているゲートウェイのアドレスを、ノードＤＢ１２０から特定する。

[0035] ノードＤＢ１２０は、アドホックネットワークＡ１～Ａ４内の各ノードのアドレスと各ノードが所属するアドホックネットワーク内のゲートウェイＧ１～Ｇ４の識別情報（アドレスでもよい）を関連付けたデータベースである。なお、新規ノードＮｘについては、この段階ではどのゲートウェイの配下になるか決まっていない。

[0036] （５）管理サーバ１０１は、（４）で特定されたゲートウェイＧ１～Ｇ３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。

[0037] 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。

[0038] （６）管理サーバ１０１は、ノードＤＢ１２０に新規ノードＮｘの所属ゲートウェイＧ３のアドレスを登録する。これにより、あらたな新規ノード導入に際して、新規ノードＮｘのアドレスからゲートウェイＧ３のアドレス、暗号鍵Ｋ３およびノード数を特定することができる。

[0039] （７）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。

[0040] （８）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。

[0041] （９）新規ノードＮｘ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。

[0042] 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。

[0043] また、傍受したパケットは、ゲートウェイＧ１～Ｇ３からの定期的な暗号化パケットＳＰ１～ＳＰ３をノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ経由で傍受し、傍受した暗号化パケットＳＰ１～ＳＰ３を管理サーバ１０１にネットワークＮＷ２，ＮＷ３経由で送信することも考えられる。この場合、暗号化パケットＳＰ１～ＳＰ３は、時刻同期やルーティングテーブルの配布など定期的に送信されるパケットであるため、新規ノードＮｘを設置してから暗号化パケットＳＰ１～ＳＰ３を傍受するまで、最大で暗号化パケットＳＰ１～ＳＰ３の送信間隔分待機しなければならない。

[0044] これに対し、実施の形態１では、アドホックネットワークＡ１～Ａ３内で不定期にマルチホップ通信された暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃを新規ノードＮｘが傍受する。したがって、傍受するまでの期間の短縮化を図ることができ、新規ノードＮｘの導入処理を早期に完了することができる。

[0045] 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。

[0046] （ネットワークシステム１００の一実施例）

図２は、実施の形態１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。

[0047] 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。

[0048] ここで、管理サーバ１０１は、暗号鍵ＤＢ１１０とノードＤＢ１２０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。

[0049] 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。

[0050] 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。

[0051] 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。

[0052] 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。

[0053] 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。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] （管理サーバ１０１のハードウェア構成例）

図３は、実施の形態１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。

[0058] 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。

[0059] 光ディスクドライブ３０６は、ＣＰＵ３０１の制御に従って光ディスク３０７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。

[0060] 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。

[0061] 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。

[0062] 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。

[0063] （ノードのハードウェア構成例）

図４は、実施の形態１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。

[0064] 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、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。

[0065] 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。

[0066] （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。

[0067] 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。

[0068] 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。

[0069] 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。

[0070] （ノードＤＢ１２０の記憶内容）

図６は、図１に示したノードＤＢ１２０の記憶内容の一例を示す説明図である。図６において、ノードＤＢ１２０は、ノードアドレスと所属ゲートウェイ（所属GW）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、ノードごとの所属ＧＷのＩＤ（図５のＩＤに相当）をレコードとして記憶している。

[0071] ここでは、たとえば、『ａａ：ａａ：ａａ：ａａ：ａａ：ａａ』をアドホックネットワークＡ１内のノードＮ１ａのアドレスとしている。また、『ｂｂ：ｂｂ：ｂｂ：ｂｂ：ｂｂ：ｂｂ』をアドホックネットワークＡ２内のノードＮ２ｂのアドレスとしている。また、『ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ』をアドホックネットワークＡ３内のノードＮ３ｃのアドレスとしている。また、『ｄｄ：ｄｄ：ｄｄ：ｄｄ：ｄｄ：ｄｄ』をアドホックネットワークＡ４内のノードＮ４ｄのアドレスとしている。

[0072] すなわち、ノードＤＢ１２０を参照することで、ノードの所属ＧＷが特定される。なお、所属ＧＷのフィールドには、所属ＧＷのＩＤの代わりに、所属ＧＷのアドレスを記憶してもよい。

[0073] （新規ノードＮｘ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Ｎｘの導入時における暗号鍵Ｋｉの設定例について説明する。

[0074] 図７は、実施の形態１にかかる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７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７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。

[0075] 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１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内の新規ノードＮｘ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Ｎｘに自動設定する。

[0076] 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。

[0077] 図８は、実施の形態１にかかる新規ノード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８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。

[0078] 図８のシーケンスにおいて、（１）ゲートウェイＧｉは、アドホックネットワークＡｉのネットワーク情報を管理サーバ１０１に送信する。ネットワーク情報は、ゲートウェイＧｉ固有の暗号鍵Ｋｉとアドホックネットワーク Ａｉ内のノードＮｉ－１～Ｎｉ－３のアドレスを含む。ゲートウェイＧｉは、アドホックネットワークＡｉ内のマルチホップ通信で事前にノードＮｉ－１～Ｎｉ－３のアドレスを取得してあるため、ネットワーク情報に含めて管理サーバ１０１に送信することができる。

[0079] （２）管理サーバ１０１は、ネットワーク情報からゲートウェイＧｉ固有の暗号鍵Ｋｉを取り出して、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。

[0080] （３）管理サーバ１０１は、ネットワーク情報からノードＮｉ－１～Ｎｉ－３のアドレスを取り出して、ノードＮｉ－１～Ｎｉ－３のアドレスとゲートウェイＧｉのＩＤとを関連付けてノードＤＢ１２０に登録する。なお、上記（１）～（３）の処理はおこなわず、あらかじめ暗号鍵ＤＢ１１０およびノードＤＢ１２０を、上記（２）および（３）での登録状態にしておいてもよい。

[0081] （４）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。ゲートウェイＧｉからの暗号化パケットＳＰｉは、アドホックネットワークＡｉ内の時刻

同期などアドホックネットワークＡｉ内の全ノードに通知するために周期的（たとえば、１時間に１回）に通知されるパケットである。また、設定初期化や、上述したアドホックネットワークＡｉ内のルーティング設定など一時的に送信されるパケットでもよい。

[0082] （５）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に転送する。具体的には、ノードＮｉ－１には、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設定された、転送元アドレスと転送先アドレスを関連付けたルーティングテーブルＲｉ－１がある。たとえば、図８では、転送元アドレス：ゲートウェイＧｉのアドレス、転送先アドレス：ノードＮｉ－３のアドレスと規定されているため、暗号化パケットＳＰｉは、ノードＮｉ－３に転送される。

[0083] ノードＮｉ－３にも、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設定された、転送元アドレスと転送先アドレスを関連付けたルーティングテーブルＲｉ－３がある。たとえば、図８では、転送元アドレス：ノードＮｉ－１のアドレス、転送先アドレス：－（なし）と規定されているため、暗号化パケットＳＰｉは、どこにも転送されない。これにより、ブロードキャストパケットである暗号化パケットＳＰｉが末端ノードであるノードＮｉ－３にまで行き渡る。

[0084] （６）また、ノードＮｉ－１は、自ノードで計測データが得られた場合、ゲートウェイＧｉ固有の暗号鍵Ｋｉで暗号化された暗号化パケットＳＰｉ１を、ルーティングテーブルＲｉ－１に従ってゲートウェイＧｉに送信する。暗号化パケットＳＰｉ１は、たとえば、ノードＮｉ－１での計測データを暗号鍵Ｋｉで暗号化したパケットである。暗号化パケットＳＰｉ１は、送信元アドレスをノードＮｉ－１のアドレス、宛先アドレスをゲートウェイＧｉのアドレスとするユニキャストパケットである。

[0085] （７）同様に、ノードＮｉ－３は、自ノードで計測データが得られた場合、ゲートウェイＧｉ固有の暗号鍵Ｋｉで暗号化された暗号化パケットＳＰｉ３を、ルーティングテーブルＲｉ－３に従ってノードＮｉ－１に送信する。

暗号化パケットＳＰｉ３は、たとえば、ノードＮｉ－３での計測データを暗号鍵Ｋｉで暗号化したパケットである。暗号化パケットＳＰｉ３は、送信元アドレスをノードＮｉ－３のアドレス、宛先アドレスをゲートウェイＧｉのアドレスとするユニキャストパケットである。

[0086] （８）ノードＮｉ－１は、ゲートウェイＧｉ固有の暗号鍵Ｋｉで暗号化された暗号化パケットＳＰｉ３を、ルーティングテーブルＲｉ－１に従ってゲートウェイＧｉに転送する。

[0087] なお、ノードＮｉ－１，Ｎｉ－３からの暗号化パケットＳＰｉ１，ＳＰｉ３は、ゲートウェイＧｉのブロードキャストパケット（暗号化パケットＳＰｉ）の送信周期よりも短い周期で送信されるパケットである。たとえば、各ノードＮｉ－１，Ｎｉ－３内では、ゲートウェイＧｉのブロードキャストパケット（暗号化パケットＳＰｉ）の送信周期よりも短い周期で計測データが得られる。

[0088] そのため、ノードＮｉ－１，Ｎｉ－３は、計測データが得られる都度、ゲートウェイＧｉに計測データを含む暗号化パケットＳＰｉ１，ＳＰｉ３をマルチホップ通信することとなる。そして、ゲートウェイＧｉは、ノードＮｉ－１，Ｎｉ－３からの暗号化パケットＳＰｉ１，ＳＰｉ３を管理サーバ１０１に送信することで、ノードＮｉ－１，Ｎｉ－３の時系列な計測データを得ることができる。

[0089] そして、上記（４）のブロードキャストパケット（暗号化パケットＳＰｉ）の送信後に、新規ノードＮｘがノードＮｉ－３の通信圏内に設置されたとする。新規ノードＮｘは設置しただけではゲートウェイＧｉ固有の暗号鍵Ｋｉを有していないため、暗号鍵Ｋｉで暗号化されたパケットを受信できても復号はできない状態である。

[0090] また、新規ノードＮｘは、暗号鍵Ｋｉを有していないため、新規ノードＮｘでの計測データを暗号化することができず、パケット送信しても送信先のノードに受信してもらえない状態である。また、ノードＤＢ１２０には、新規ノードＮｘの所属ＧＷが登録されていない。

[0091] （９）そして、上記（７）において、ノードＮｉ－３から送信された暗号化パケットＳＰｉ３は、ルーティングテーブルＲｉ－３で新規ノードＮｘが転送先でないにもかかわらず、新規ノードＮｘに傍受される。

[0092] （１０）新規ノードＮｘは、ノードＮｉ－３から傍受した暗号化パケットＳＰｉ３から、暗号化パケットＳＰｉ３のヘッダ部に記述されている送信元アドレス（ノードＮｉ－３のアドレス）を抽出する。暗号化パケットＳＰｉ３のヘッダ部は暗号化されていないため、新規ノードＮｘは、送信元アドレス（ノードＮｉ－３のアドレス）を抽出することができる。

[0093] なお、上述した（１）～（１０）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は近隣ノードからの暗号化パケット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。つぎに、図９のシーケンスに移る。

[0094] 図９は、実施の形態１にかかる新規ノード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９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。

[0095] （１１）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１４および図１５を用いて後述する。

[0096] （１２）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Ｎｘとを接続することで、携帯端末ＭＴと新規ノードＮｘとの間にネットワークＮＷ３が確立される。

[0097] （１３）新規ノードＮｘは、ネットワークＮＷ３を介して、図８に示した（１０）において抽出されたノードＮｉ－３のアドレスのように、近隣ノードから傍受した暗号化パケットから抽出されたアドレスをまとめたアドレスリスト１３０を生成する。アドレスリスト１３０には、新規ノードＮｘのアドレスも含まれているものとする。

[0098] （１４）新規ノードＮｘは、アドレスリスト１３０を含むパケットＰＮを携帯端末ＭＴに送信する。

[0099] （１５）携帯端末ＭＴは、ネットワークＮＷ２を介して、新規ノードＮｘからのパケットＰＮを管理サーバ１０１に送信する。

[0100] （１６）管理サーバ１０１は、携帯端末ＭＴからのパケットＰＮを受信し、パケットＰＮに含まれているアドレスリスト１３０内のノードのアドレスを抽出する。そして、管理サーバ１０１は、ノードＤＢ１２０を参照して、抽出されたノードのアドレスと関連付けて記憶されている所属ＧＷのＩＤ（または所属ＧＷのアドレス）を特定する。

[0101] （１７）管理サーバ１０１は、上記（１６）で特定された各所属ＧＷ配下のノード数を、暗号鍵ＤＢ１１０から特定する。

[0102] （１８）管理サーバ１０１は、上記（１７）で特定された各所属ＧＷ配下のノード数の中から最大ノード数でないノード数である所属ＧＷを特定する。そして、管理サーバ１０１は、この特定された所属ＧＷのＩＤ（または所属ＧＷのアドレス）を手がかりとして、暗号鍵ＤＢ１１０の中から、ゲートウェイＧｉのＩＤ（または所属ＧＷ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。

[0103] （１９）管理サーバ１０１は、受信されたパケットＰＮに含まれている新規ノードＮｘのアドレスを、上記（１８）で選択された所属ＧＷのＩＤ（または所属ＧＷのアドレス）に関連づけて、ノードＤＢ１２０に登録する。これにより、新規ノードＮｘの所属ＧＷがゲートウェイＧｉであることが、ノードＤＢ１２０を参照することで特定可能となる。

[0104] （２０）管理サーバ１０１は、ネットワークＮＷ２を介して、上記（１８

）で選択された暗号鍵Ｋｉ（選択鍵Ｋｓ）を携帯端末ＭＴに送信する。送信のタイミングは、上記（１９）の前でも後でもよい。（１９）の前に送信する場合は、（１９）のノードＤＢ１２０の更新を待たずして、新規ノードＮｘの設定処理を実行できるため、設定処理の高速化を図ることができる。

[0105] （２１）管理サーバ１０１は、暗号鍵ＤＢ１１０において、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。

[0106] （２２）携帯端末ＭＴは、ネットワークＮＷ３を介して、管理サーバ１０１からの選択鍵Ｋｓを新規ノードＮｘに送信する。

[0107] （２３）新規ノードＮｘは、携帯端末ＭＴからの選択鍵Ｋｓを、パケットを暗号化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で暗号化パケットを送信したり、選択鍵Ｋｓで暗号化された暗号化パケットを受信した場合に選択鍵Ｋｓで復号することができる。

[0108] （２４）このあと、新規ノードＮｘは復号確認をおこなってもよい。具体的には、新規ノードＮｘは、図８の（９）において、近隣ノードからの暗号化ＳＰｉ３を傍受して保持している。

[0109] したがって、新規ノードＮｘは、上記（２３）で受信した選択鍵Ｋｓで、暗号化パケットＳＰｉ３の復号を試みる。復号が成功した場合は、そのまま新規ノードＮｘは選択鍵Ｋｓを使用することができる。一方、復号が失敗した場合は、再度（１０）～（２３）を実行することとなる。この場合、上記（２１）でインクリメントされたノード数は元に戻される。また、上記（２１）は、管理サーバ１０１が（２４）の復号確認の通知を新規ノードＮｘから受信したあとに実行することとしてもよい。

[0110] このように、新規ノードＮｘ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近隣ノードのアドレス群を手掛かりに、携帯端末ＭＴを介して、管理サーバ１０１に鍵要求することで、設定すべき暗号鍵Ｋｉを取得することができる。

[0111] すなわち、既設定のノードは常時、計測データを暗号化パケットとしてゲートウェイＧｉを宛先として送信しているため、新規ノードＮｘの設置時に

おいて早期に上記（９）～（２４）の処理を実行することが可能となる。したがって、作業員ＯＰは、ブロードキャストパケット（暗号化パケットＳＰｉ）で設定作業をおこなう場合にくらべて、設定作業を円滑におこなうことができる。

[0112] 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。

[0113] （ノードＮの機能的構成例）

図１０は、ノードの機能的構成例を示すブロック図である。図１０において、ノードＮは、パケット受信部１００１と、検知部１００２と、パケット送信部１００３と、鍵受信部１００４と、設定部１００５と、抽出部１００６と、生成部１００７と、復号部１００８と、出力部１００９と、取得部１０１０と、暗号化処理部１０１１と、を含む構成である。

[0114] 各機能部（パケット受信部１００１～暗号化処理部１０１１）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１００１～暗号化処理部１０１１）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。

[0115] パケット受信部１００１は、アドホックネットワークＡｉ内からの暗号化パケットを受信する。暗号化パケットは、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、暗号化パケットは、図１に示したような近隣ノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃからの暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃであったり、ゲートウェイＧ１～Ｇ３からブロードキャストされた暗号化パケットＳＰ１～ＳＰ３である。以降、近隣ノ

ードからの暗号化パケットを、「暗号化パケットＳＰｉｙ」と称す。ここで、暗号化パケットＳＰｉｙのデータ構造について説明する。

[0116] 図１１は、暗号化パケットＳＰｉｙのデータ構造の一例を示す説明図である。図１１において、暗号化パケットＳＰｉｙは、ヘッダ部１１１０とペイロード部１１２０とを含む構成である。ヘッダ部１１１０には、宛先アドレス、差出アドレス、ホップ数が記述されている。ペイロード部１１２０には、暗号化されたデータ本体が記述されている（図１１中ハッチ部分）。

[0117] ここで、宛先アドレスは、送信先のアドレスである。差出アドレスは、送信元のアドレスである。また、ヘッダ部１１１０にはゲートウェイＧｉのアドレスが記述されている。図１１では、暗号化パケットＳＰｉｙを暗号化パケットＳＰ３ｃ（図１参照）としているため、宛先アドレスは、ゲートウェイＧｉのアドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：９０：１２』であり、差出アドレスは、ノードＮ３ｃのアドレス『ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ』である。

[0118] なお、暗号化パケットＳＰｉｙが暗号化パケットＳＰｉ（ゲートウェイＧｉからのブロードキャストパケット）の場合、宛先アドレスは、ブロードキャスト用のＭＡＣアドレス『００：００：００：００：００：００』となる。また、ここでは宛先アドレスおよび差出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。

[0119] ホップ数は、マルチホップの上限回数であり、マルチホップされる都度、デクリメントされる。図１０では、『１０』となっているため、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。

[0120] 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１００１は、近隣ノードからの暗号化パケットＳＰｉｙを受信（傍受）する。また、パケット受信部１００１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、転送先でない場合は、通信圏内であれば暗号化パケットＳＰｉｙを傍受する。

[0121] 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ＳＰｉｙ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ＳＰｉｙは、傍受したノードＮで破棄されることとなる。なお、暗号鍵の設定処理が完了するまでは傍受したパケットを破棄せずに保持しておくこととしてもよい。

[0122] 検知部１００２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１００２が、ＵＳＢケーブルを介した携帯端末ＭＴとの接続を検知する。

[0123] 抽出部１００６は、受信された暗号化パケットＳＰｉｙから近隣ノードのアドレスを抽出する。すなわち、具体的には、たとえば、新規ノードＮｘの場合は、抽出部１００６は、図１１に示した暗号化パケットＳＰｉｙのヘッダ部１１１０の差出アドレスを抽出する。図１１の例では、抽出部１００６は、ノードＮ３ｃのアドレス『ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ』を抽出する。

[0124] 生成部１００７は、パケットＰＮを生成する。具体的には、たとえば、生成部１００７は、抽出部１００６によって抽出された近隣ノードのアドレス（暗号化パケットＳＰｉｙの差出アドレス）および新規ノード（自ノード）Ｎｘのアドレスを並べたアドレスリスト１３０を生成する。そして、生成部１００７は、生成されたアドレスリスト１３０を含むパケットＰＮを生成する。なお、新規ノードＮｘのアドレスはパケットＰＮの差出アドレスとして記述されるため、アドレスリスト１３０に含めなくてもよい。

[0125] パケット送信部１００３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、パケットＰＮ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１００３が、ＵＳＢケーブルなどのネットワークＮＷ３を介して、パケットＰＮ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、新規ノードＮｘからのパケットＰＮを管理サーバ１０１に送信する。また、パケット送信部１００３

は、選択鍵Ｋｓが設定されたあとは、選択鍵Ｋｓで暗号化された暗号化パケットを宛先（たとえば、所属ＧＷ）に送信する。

[0126] 鍵受信部１００４は、携帯端末ＭＴを介して、選択鍵Ｋｓを管理サーバ１０１から受信する。選択鍵Ｋｓは、たとえば、パケットを暗号化するとともに、選択鍵Ｋｓを用いて暗号化された暗号化パケットを復号することができる共通鍵である。

[0127] 設定部１００５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１００５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。

[0128] 復号部１００８は、設定処理中において、設定部１００５によって設定された暗号鍵Ｋｉで、パケット受信部１００１によって受信された暗号化パケットＳＰｉｙの復号を試みる。すなわち、復号部１００８は、抽出部１００６によって近隣ノードのアドレスの抽出対象となった暗号化パケット（ＳＰ３ｃ）の復号を試みる。また、復号部１００８は、選択鍵Ｋｓが設定された後、設定部１００５によって設定された選択鍵Ｋｓで、パケット受信部１００１によって受信される暗号化パケットＳＰｉｙを復号する。

[0129] また、復号の成否は、暗号化パケットＳＰｉｙ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、暗号化パケットＳＰｉｙを復号し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、復号部１００８は、暗号化パケットＳＰｉｙの復号が成功したと判断する。

[0130] 出力部１００９は、復号部１００８による復号結果を出力する。具体的には、たとえば、出力部１００９は、差出アドレスの抽出対象となった暗号化

パケット（ＳＰ３ｃ）の復号が成功した場合、成功した旨をディスプレイに表示したり、音声により報知する。また、出力部１００９は、差出アドレスの抽出対象となった暗号化パケット（ＳＰ３ｃ）の復号が失敗した場合、失敗した旨をディスプレイに表示したり、音声により報知する。

[0131] 取得部１０１０は、計測対象で測定された測定データを取得する。たとえば、ノードＮが電力計に内蔵または接続されている場合は、電力量を取得することとなる。暗号化処理部１０１１は、取得部１０１０によって取得されたデータを、選択鍵Ｋｓで暗号化する。これにより、パケット送信部１００３は、暗号化パケットＳＰｉｙを所属ＧＷに送信することができる。

[0132] （管理サーバ１０１の機能的構成）

図１２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１２において、管理サーバ１０１は、受信部１２０１と、特定部１２０２と、更新部１２０３と、選択部１２０４と、送信部１２０５と、を含む構成である。各機能部（受信部１２０１～送信部１２０５）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／Ｆ３０８により、その機能を実現する。また、各機能部（受信部１２０１～送信部１２０５）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。

[0133] 受信部１２０１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１２０１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。

[0134] 特定部１２０２は、受信部１２０１によって受信されたパケットＰＮから、パケットＰＮに含まれている近隣ノードのアドレスを抽出する。そして、特定部１２０２は、抽出された近隣ノードのアドレスに関連づけて記憶されている所属ＧＷのＩＤを、ノードＤＢ１２０から特定する。たとえば、パケ

ットＰＮのペイロード部１１２０にノードＮ１ａのアドレス『ａａ：ａａ：ａａ：ａａ：ａａ：ａａ』が含まれている場合、所属ＧＷのＩＤ：Ｇ１が特定される。

[0135] また、パケットＰＮのペイロード部１１２０にノードＮ２ｂのアドレス『ｂｂ：ｂｂ：ｂｂ：ｂｂ：ｂｂ：ｂｂ』が含まれている場合、所属ＧＷのＩＤ：Ｇ２が特定される。また、パケットＰＮのペイロード部１１２０にノードＮ３ｃのアドレス『ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ：ｃｃ』が含まれている場合、所属ＧＷのＩＤ：Ｇ３が特定される。

[0136] また、特定部１２０２は、特定された所属ＧＷのＩＤに関連付けられているノード数を、暗号鍵ＤＢ１１０から特定する。具体的には、たとえば、所属ＧＷのＩＤとしてＧ１～Ｇ３が特定された場合、特定部１２０２は、所属ＧＷ：Ｇ１のノード数：１０、所属ＧＷ：Ｇ２のノード数：５、所属ＧＷ：Ｇ３のノード数：３を特定する。

[0137] 更新部１２０３は、受信部１２０１によって受信されたパケットＰＮから、パケットＰＮに含まれている新規ノードＮｘのアドレスを抽出する。そして、後述する選択部１２０４で選択された暗号鍵Ｋｉに関連付けられているＧＷのＩＤを、抽出した新規ノードＮｘのアドレスに関連付けてノードＤＢ１２０に登録する。これにより、ノードＤＢ１２０が更新される。ここで、更新の具体例について説明する。

[0138] 図１３は、ノードＤＢ１２０の更新の具体例を示す説明図である。具体的には、たとえば、新規ノードがノードＮｘの場合、更新部１２０３は、ノードＮｘのアドレス『ｘｘ：ｘｘ：ｘｘ：ｘｘ：ｘｘ：ｘｘ』を、特定部１２０２によって特定された所属ＧＷのＩＤ：Ｇ３に関連づけて、レコードを追加登録する。これにより、ノードＤＢ１２０が更新されることとなる。

[0139] また、図１２に戻り、選択部１２０４は、暗号鍵ＤＢ１１０の中から、特定した所属ＧＷのうち、ノード数が最大ではない所属ＧＷ固有の暗号鍵Ｋｉを選択鍵Ｋｓとして選択する。上述した例では、ノード数「１０」が最大であるため、所属ＧＷ：Ｇ２，Ｇ３のうちいずれかに固有の暗号鍵Ｋｉを選択

鍵Ｋｓとして選択する。選択部１２０４は、選択対象となった暗号鍵Ｋｉを暗号鍵ＤＢ１１０から抽出する。

[0140] この場合、特定されたノード数のうち最小ノード数の所属ＧＷ固有の暗号鍵Ｋｉ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１２０４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。

[0141] なお、選択部１２０４は、特定部１２０２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１２０４は、特定部１２０２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。

[0142] 送信部１２０５は、携帯端末ＭＴを介して、選択鍵Ｋｓを、受信されたパケットに含まれている新規ノードＮｘのアドレス宛に送信する。具体的には、たとえば、送信部１２０５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。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を新規ノードＮｘに送信する。

[0143] なお、上述した説明では、管理サーバ１０１がパケットＰＮ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、パケットＰＮ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１２０４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。

[0144] （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。

[0145] 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ＲＡＭ３０３やフラッシュメモリなどの記憶装置に記憶される。

[0146] 図１４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１４において、管理サーバ１０１の認証情報１４００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。

[0147] 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。

[0148] 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１５に示すような携帯端末ＭＴの認証情報１５００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。

[0149] 図１５は、携帯端末ＭＴの認証情報の一例を示す説明図である。図１５において、携帯端末ＭＴの認証情報１５００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。

[0150] 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。

[0151] 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。

[0152] 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。認証情報１５００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。

[0153] （ノードＮの鍵設定処理手順）

図１６は、実施の形態１にかかる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１００１により、近隣ノードからの暗号化パケットＳＰｉｙを受信したか否かを判断する（ステップＳ１６０１）。たとえば、新規ノードＮｘが、近隣ノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃからの暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃを受信（傍受）したか否かを判断する。

[0154] ここで、暗号化パケットＳＰｉｙを受信（傍受）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）、ノードＮは、受信（傍受）した暗号化パケットＳＰｉｙから近隣ノードのアドレスを抽出する（ステップＳ１６０２）。そして、ノードＮは、抽出された近隣ノードのアドレスと自ノードＮのアドレスを含むパケットＰＮを生成する（ステップＳ１６０３）。このあと、ノードＮは、検知部１００２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Ｓ１６０４）。

[0155] ここで、ノードＮは、携帯端末ＭＴとの接続が検知されるのを待って（ス

テップＳ１６０４：Ｎｏ）、検知された場合（ステップＳ１６０４：Ｙｅｓ）、パケット送信部１００３により、携帯端末ＭＴを介して、生成パケットＰＮを管理サーバ１０１に送信する（ステップＳ１６０５）。

[0156] このあと、ノードＮは、鍵受信部１００４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Ｓ１６０６）。

[0157] ここで、ノードＮは、選択鍵Ｋｓを受信するのを待って（ステップＳ１６０６：Ｎｏ）、受信した場合（ステップＳ１６０６：Ｙｅｓ）、設定部１００５により、受信されたゲートウェイＧｉ固有の選択鍵Ｋｓを、暗号化パケットＳＰｉｙを暗号化するための鍵に設定する（ステップＳ１６０７）。

[0158] このあと、ノードＮは、復号部１００８により、ステップＳ１６０１において近隣ノードから送信されてきた暗号化パケットＳＰｉｙの復号を試みる（ステップＳ１６０８）。復号が失敗した場合（ステップＳ１６０８：Ｎｏ）、ノードＮは、出力部１００９により設定エラーを出力し（ステップＳ１６０９）、ステップＳ１６０１に戻る。一方、復号が成功した場合（ステップＳ１６０８：Ｙｅｓ）、ノードＮは、出力部１００９により設定完了を出力し（ステップＳ１６１０）、本フローチャートによる一連の処理を終了する。

[0159] 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。

[0160] （管理サーバ１０１の鍵提供処理手順）

図１７は、実施の形態１にかかる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のフローチャートにおいて、まず、管理サーバ１０１は、受信部１２０１により、携帯端末ＭＴを介して、生成パケットＰＮをノードＮから受信したか否かを判断する（ステップＳ１７０１）。

[0161] ここで、生成パケットＰＮを受信するのを待って（ステップＳ１７０１：Ｎｏ）、受信した場合（ステップＳ１７０１：Ｙｅｓ）、管理サーバ１０１

は、特定部１２０２により、生成パケットＰＮの中から近隣ノードのアドレスを抽出する。そして、管理サーバ１０１は、抽出された近隣ノードのアドレスに関連付けて記憶されている所属ＧＷのＩＤを、ノードＤＢ１２０から特定する（ステップＳ１７０２）。

[0162] つぎに、管理サーバ１０１は、特定部１２０２により、ステップＳ１７０２で特定された各所属ＧＷのＩＤに関連付けられているノード数を、暗号鍵ＤＢ１１０から特定する（ステップＳ１７０３）。そして、管理サーバ１０１は、選択部１２０４により、ステップＳ１７０３で特定された所属ＧＷごとのノード数に基づいて、最大ノード数以外のノード数となるいずれかの所属ＧＷ固有の暗号鍵Ｋｉを、選択鍵Ｋｓとして選択する（ステップＳ１７０４）。

[0163] このあと、管理サーバ１０１は、更新部１２０３により、生成パケットＰＮから送信元のノードＮのアドレスを抽出し、選択鍵Ｋｓに関連付けられている所属ＧＷのＩＤと関連付けて、ノードＤＢ１２０に登録する（ステップＳ１７０５）。これにより、ノードＮの登録後に、ノードＮが新規ノードの近隣ノードになった場合でも、新規ノードＮｘの所属ＧＷを特定することができる。

[0164] また、管理サーバ１０１は、送信部１２０５により、携帯端末ＭＴを介して、選択鍵Ｋｓをノードに送信する（ステップＳ１７０６）。このあと、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Ｓ１７０７）、本フローチャートによる一連の処理を終了する。

[0165] 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。

[0166] 以上説明したように、本実施の形態１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、近隣ノードからの暗号化パケ

ットＳＰｉｙ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、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。

[0167] 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近隣ノードからの暗号化パケットＳＰｉｙ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。

[0168] また、本実施の形態１によれば、ノードＮは、近隣ノードからの暗号化パケットＳＰｉｙ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。

[0169] 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。

[0170] ＜実施の形態２＞

つぎに、実施の形態２について説明する。上述した実施の形態１では、各近隣ノードのアドレスに関連付けられている所属ＧＷをそれぞれ特定し、特定した各所属ＧＷに関連付けられているノード数により、選択鍵Ｋｓを選択した。これに対し、実施の形態２では、さらに、各所属ＧＷ配下の隣接ノー

ドのアドレス数を考慮する。所属ＧW配下の隣接ノードのアドレス数が多いアドホックネットワークＡｉに所属させた場合、マルチホップ通信相手が多くなる。したがって、新規ノードは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。

[0171] また、所属ＧW配下の隣接ノードのアドレス数が少ないアドホックネットワークＡｉに所属させた場合、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。以下、所属ＧW配下の隣接ノードのアドレス数を考慮した場合について、詳細に説明する。

[0172] （ネットワークシステムでのノード数平均化例）

図１８は、実施の形態２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。なお、図１に示した構成と同一構成については同一符号を付し、その説明を省略する。

[0173] 図１８において、ノードＮ１ｅはアドホックネットワークＡ１内のノードであり、ゲートウェイＧ１固有の暗号鍵Ｋ１を有する。また、ノードＮ２ｆはアドホックネットワークＡ２内のノードであり、ゲートウェイＧ２固有の暗号鍵Ｋ２を有する。暗号化パケットＳＰ１ｅ，ＳＰ２ｆは、ノードＮ１ｅ，Ｎ２ｆからそれぞれマルチホップ通信で送信されるパケットである。また、アドホックネットワークＡ３のノード数を「５」とする。以下、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。

[0174] （１）まず、新規ノードＮｘは、暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ１ｅ，ＳＰ２ｆを傍受する。暗号化パケットＳＰ４ｄは通信圏外であるため、傍受できない。

[0175] （２）新規ノードＮｘは、傍受した暗号化パケットＳＰ１ａ，ＳＰ２ｂ，ＳＰ３ｃ，ＳＰ１ｅ，ＳＰ２ｆから傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ１ｅ，Ｎ２ｆのアドレスを抽出し、アドレスリスト１３０を生成する。

[0176] （３）新規ノードＮｘは、上記（２）で生成されたアドレスリスト１３０を

含むパケットＰＮを携帯端末ＭＴ経由で管理サーバ１０１に送信する。なお、パケットＰＮには、新規ノードＮｘのアドレスも含ませる。

[0177] （４）管理サーバ１０１は、新規ノードＮｘからパケットＰＮを受信すると、パケットＰＮを解析して、パケットＰＮに含まれている傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ１ｅ，Ｎ２ｆのアドレスと新規ノードＮｘのアドレスを抽出する。そして、管理サーバ１０１は、抽出された傍受元のノードＮ１ａ，Ｎ２ｂ，Ｎ３ｃ，Ｎ１ｅ，Ｎ２ｆのアドレスに関連付けされているゲートウェイのアドレスを、ノードＤＢ１２０から特定する。

[0178] （５）また、管理サーバ１０１は、特定された所属ＧＷごとに、パケットＰＮから抽出された傍受元のノードのアドレス数を計数する。たとえば、所属ＧＷ：Ｇ１については、傍受元のノードＮ１ａ，Ｎ１ｅのアドレスで特定されたため、計数されたアドレス数（以下、「カウント数」）は、「２」である。また、所属ＧＷ：Ｇ２については、傍受元のノードＮ２ｂ，Ｎ２ｆのアドレスで特定されたため、計数されたアドレス数（カウント数）は、「２」である。また、所属ＧＷ：Ｇ３については、傍受元のノードＮ３ｃのアドレスで特定されたため、カウント数は、「１」である。

[0179] （６）管理サーバ１０１は、（４）で特定されたゲートウェイＧ１～Ｇ３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（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のノード数と（５）で得られたカウント数とにより、選択鍵Ｋｓを決定する。具体的には、ノード数が最大ではない所属ゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵として選択するが、最大ノード数以外のノード数が同数の場合、カウント数の大きさで選択する。

[0180] たとえば、（４）で特定された所属ゲートウェイＧ１～Ｇ３のうち最大ノード数の所属ゲートウェイＧ１以外の所属ゲートウェイＧ２，Ｇ３のノード数は同数（５個）である。所属ゲートウェイＧ２のカウント数は「２」、所属ゲートウェイＧ３のカウント数は「１」である。そのため、管理サーバ１

０１は、カウント数の大きい所属ゲートウェイＧ２固有の暗号鍵Ｋ２を選択鍵Ｋｓとして選択し、暗号鍵ＤＢ１１０から抽出する。

[0181] （７）管理サーバ１０１は、ノードＤＢ１２０に新規ノードＮｘの所属ゲートウェイＧ３のアドレスを登録する。これにより、あらたな新規ノード導入に際して、新規ノードＮｘのアドレスからゲートウェイＧ２のアドレス、暗号鍵Ｋ２およびノード数を特定することができる。

[0182] （８）管理サーバ１０１は、選択鍵Ｋ２を、携帯端末ＭＴを介して新規ノードＮｘに送信する。

[0183] （９）管理サーバ１０１は、暗号鍵Ｋ２に関連付けられているノード数を「５」から「６」に更新する。

[0184] （１０）新規ノードＮｘは、管理サーバ１０１からの選択鍵Ｋ２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。

[0185] このように、実施の形態２では、実施の形態１にさらにカウント数を考慮することで、アドホックネットワークＡ１～Ａ４のノード数の平均化を図りつつ、近隣ノード数の多いアドホックネットワークＡｉに優先的に新規ノードＮｘを導入することができる。

[0186] 図１９は、実施の形態２にかかる新規ノード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１９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。なお、前半のシーケンスは図８と同一であるため省略する。

[0187] （１１）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１４および図１５と同一である。

[0188] （１２）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

ケーブルを用いて、携帯端末ＭＴと新規ノードＮｘとを接続することで、携帯端末ＭＴと新規ノードＮｘとの間にネットワークＮＷ３が確立される。

[0189] （１３）新規ノードＮｘは、ネットワークＮＷ３を介して、図８に示した（１０）において抽出されたノードＮｉ－３のアドレスのように、近隣ノードから傍受した暗号化パケットから抽出されたアドレスをまとめたアドレスリスト１３０を生成する。アドレスリスト１３０には、新規ノードＮｘのアドレスも含まれているものとする。

[0190] （１４）新規ノードＮｘは、アドレスリスト１３０を含むパケットＰＮを携帯端末ＭＴに送信する。

[0191] （１５）携帯端末ＭＴは、ネットワークＮＷ２を介して、新規ノードＮｘからのパケットＰＮを管理サーバ１０１に送信する。

[0192] （１６）管理サーバ１０１は、携帯端末ＭＴからのパケットＰＮを受信し、パケットＰＮに含まれているアドレスリスト１３０内のノードＮのアドレスを抽出する。そして、管理サーバ１０１は、ノードＤＢ１２０を参照して、抽出されたノードのアドレスと関連付けて記憶されている所属ＧＷのＩＤ（または所属ＧＷのアドレス）を特定する。

[0193] （１７）管理サーバ１０１は、上記（１６）で特定された所属ＧＷごとにパケットＰＮに含まれている近隣ノードのアドレス数（カウント数）を計数する。

[0194] （１８）管理サーバ１０１は、上記（１６）で特定された各所属ＧＷ配下のノード数を、暗号鍵ＤＢ１１０から特定する。

[0195] （１９）管理サーバ１０１は、上記（１８）で特定された各所属ＧＷ配下のノード数の中から最大ノード数でないノード数である所属ＧＷを特定する。管理サーバ１０１は、特定された所属ＧＷのカウント数のうち最大カウント数の所属ＧＷのＩＤ（または所属ＧＷのアドレス）を特定する。そして、管理サーバ１０１は、最大カウント数の所属ＧＷのＩＤを手がかりとして、暗号鍵ＤＢ１１０の中から、最大カウント数の所属ＧＷのＩＤ（または所属ＧＷ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。

[0196] （２０）管理サーバ１０１は、受信されたパケットＰＮに含まれている新規ノードＮｘのアドレスを、上記（１９）で選択された所属ＧＷのＩＤ（または所属ＧＷのアドレス）に関連づけて、ノードＤＢ１２０に登録する。これにより、新規ノードＮｘの所属ＧＷがゲートウェイＧｉであることが、ノードＤＢ１２０を参照することで特定可能となる。

[0197] （２１）管理サーバ１０１は、ネットワークＮＷ２を介して、上記（１９）で選択された暗号鍵Ｋｉ（選択鍵Ｋｓ）を携帯端末ＭＴに送信する。送信のタイミングは、上記（２０）の前でも後でもよい。（２０）の前に送信する場合は、（２０）のノードＤＢ１２０の更新を待たずして、新規ノードＮｘの設定処理を実行できるため、設定処理の高速化を図ることができる。

[0198] （２２）管理サーバ１０１は、暗号鍵ＤＢ１１０において、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。

[0199] （２３）携帯端末ＭＴは、ネットワークＮＷ３を介して、管理サーバ１０１からの選択鍵Ｋｓを新規ノードＮｘに送信する。

[0200] （２４）新規ノードＮｘは、携帯端末ＭＴからの選択鍵Ｋｓを、パケットを暗号化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で暗号化パケットを送信したり、選択鍵Ｋｓで暗号化された暗号化パケットを受信した場合に選択鍵Ｋｓで復号することができる。

[0201] （２５）このあと、新規ノードＮｘは復号確認をおこなってもよい。具体的には、新規ノードＮｘは、図８の（９）において、近隣ノードからの暗号化ＳＰｉ３を傍受して保持している。

[0202] したがって、新規ノードＮｘは、上記（２４）で受信した選択鍵Ｋｓで、暗号化パケットＳＰｉ３の復号を試みる。復号が成功した場合は、そのまま新規ノードＮｘは選択鍵Ｋｓを使用することができる。一方、復号が失敗した場合は、再度（１０）～（２４）を実行することとなる。この場合、上記（２２）でインクリメントされたノード数は元に戻される。また、上記（２２）は、管理サーバ１０１が（２５）の復号確認の通知を新規ノードＮｘから受信したあとに実行することとしてもよい。

[0203] このように、新規ノードＮｘ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近隣ノードのアドレス群を手掛かりに、携帯端末ＭＴを介して、管理サーバ１０１に鍵要求することで、設定すべき暗号鍵Ｋｉを取得することができる。

[0204] すなわち、既設定のノードは常時、計測データを暗号化パケットとしてゲートウェイＧｉを宛先として送信しているため、新規ノードＮｘの設置時において早期に上記（９）～（２５）の処理を実行することが可能となる。したがって、作業員ＯＰは、ブロードキャストパケット（暗号化パケットＳＰｉ）で設定作業をおこなう場合にくらべて、設定作業を円滑におこなうことができる。

[0205] このように、実施の形態２では、実施の形態１にさらにカウント数を考慮することで、アドホックネットワークＡ１～Ａ４のノード数の平均化を図りつつ、近隣ノード数の多いアドホックネットワークＡｉに優先的に新規ノードＮｘを導入することができる。

[0206] （管理サーバ１０１の鍵提供処理手順）

図２０は、実施の形態２にかかる管理サーバ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。ノードＮの鍵設定処理手順については、実施の形態１（図１６）と同様なので省略する。図２０のフローチャートにおいて、まず、管理サーバ１０１は、受信部１２０１により、携帯端末ＭＴを介して、生成パケットＰＮをノードＮから受信したか否かを判断する（ステップＳ２００１）。

[0207] ここで、生成パケットＰＮを受信するのを待って（ステップＳ２００１：Ｎｏ）、受信した場合（ステップＳ２００１：Ｙｅｓ）、管理サーバ１０１は、特定部１２０２により、生成パケットＰＮの中から近隣ノードのアドレスを抽出する。そして、管理サーバ１０１は、抽出された近隣ノードのアドレスに関連付けて記憶されている所属ＧＷのＩＤを、ノードＤＢ１２０から特定する（ステップＳ２００２）。

[0208] つぎに、管理サーバ１０１は、特定部１２０２により、ステップＳ２００

２で特定された各所属ＧＷのＩＤに関連付けられているノード数を、暗号鍵ＤＢ１１０から特定する（ステップＳ２００３）。また、管理サーバ１０１は、特定部１２０２により、ステップＳ２００３で特定された所属ＧＷごとのカウント数を特定する（ステップＳ２００４）。

[0209] そして、管理サーバ１０１は、選択部１２０４により、ステップＳ２００３で特定された所属ＧＷごとのノード数およびステップＳ２００４で特定された所属ＧＷごとのカウント数に基づいて、最大ノード数以外のノード数となるいずれかの所属ＧＷ固有の暗号鍵Ｋｉを、選択鍵Ｋｓとして選択する（ステップＳ２００５）。

[0210] ここで、選択部１２０４による詳細な選択処理について説明する。ステップＳ２００３で特定された所属ＧＷごとのノード数がいずれも同数である場合は、カウント数で選択する。同様に、選択部１２０４は、ステップＳ２００３で特定された所属ＧＷごとのノード数のうち、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、カウント数で選択する。

[0211] ステップＳ２００３で特定された所属ＧＷごとのノード数がいずれも同数である場合は、選択部１２０４は、最大カウント数の所属ゲートウェイＧｉ固有の暗号鍵Ｋｉを選択鍵Ｋｓとしてもよい。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。したがって、選択部１２０４は、最大カウント数（２回）であるアドホックネットワークＡ１，Ａ２のゲートウェイＧ１，Ｇ２固有の暗号鍵Ｋ１，Ｋ２のうちいずれか一方を選択鍵Ｋｓとして抽出する。

[0212] 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、カウント数の大きさは、アドホックネットワーク内のマルチホップ通信の通信相手となる近隣ノードの多さに比例する。したがって、カウント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。

[0213] 一方、これとは逆に、カウント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１２０４は、最小カウント数（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。

[0214] 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、カウント数の大きさは、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、カウント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。

[0215] また、図１８に示したように、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（それぞれ５個）である場合、選択部１２０４は、最大カウント数（２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。

[0216] 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、カウント数の大きさは、アドホックネットワーク内のマルチホップ通信の通信相手となる近隣ノードの多さに比例する。したがって、カウント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。

[0217] 一方、これとは逆に、カウント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１２０４は、最小カウント数（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。

[0218] 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、カウント数の大きさは、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、カウント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。

[0219] 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。

[0220] このあと、管理サーバ１０１は、更新部１２０３により、生成パケットＰＮから送信元のノードＮのアドレスを抽出し、選択鍵Ｋｓに関連付けられている所属ＧＷのＩＤと関連付けて、ノードＤＢ１２０に登録する（ステップＳ２００６）。これにより、ノードＮの登録後に、ノードＮが新規ノードの近隣ノードになった場合でも、新規ノードの所属ＧＷを特定することができる。

[0221] また、管理サーバ１０１は、送信部１２０５により、携帯端末ＭＴを介して、選択鍵Ｋｓをノードに送信する（ステップＳ２００７）。このあと、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Ｓ２００８）、本フローチャートによる一連の処理を終了する。

[0222] 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。

[0223] また、カウント数の大きさを考慮することで、アドホックネットワークＡ１～Ａ４のノード数の平均化を図りつつ、近隣ノード数の多いアドホックネットワークＡｉに優先的に導入された新規ノードＮｘのマルチホップ通信の安定性の向上を図ることができる。

[0224] また、カウント数の少なさを考慮することで、アドホックネットワークＡ１～Ａ４のノード数の平均化を図りつつ、新規ノードＮｘが優先的に導入された近隣ノード数の少ないアドホックネットワークＡｉの通信経路の増強を図ることができる。

[0225] 以上説明したように、実施の形態２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、近隣ノードからの暗号化パケットＳＰｉｙ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、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。

[0226] 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近隣ノードからの暗号化パケットＳＰｉｙ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Ｋｉ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。

[0227] また、実施の形態２によれば、ノードＮは、近隣ノードからの暗号化パケットＳＰｉｙ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。

[0228] 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。

[0229] さらに、実施の形態２によれば、選択鍵Ｋｓの選択基準としてノード数のほかに、所属ＧＷごとの近隣ノードのアドレスのカウント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、カウント数の大きさは、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。

[0230] したがって、ノード数が少なく（好ましくは最小）、かつ、カウント数が大きい（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。

[0231] 一方、ノード数が少なく（好ましくは最小）、かつ、カウント数が小さい（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。

[0232] 以上のことから、実施の形態２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。

[0233] なお、上述した実施の形態２では、選択基準として所属ゲートウェイ配下のノード数を利用したり、所属ゲートウェイ配下のノード数および所属ゲートウェイ配下のノードのアドレス数（カウント数）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カウント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Ａ

ｉでは、カウント数の大きさは、アドホックネットワーク内でマルチホップ通信可能な近隣ノードの多さに比例する。

[0234] したがって、カウント数が大きい（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。

[0235] これとは逆に、カウント数が小さい（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。

[0236] また、カウント数のみ利用する場合であっても、カウント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。

[0237] 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

[0238] １００　ネットワークシステム

１０１　管理サーバ

１１０　暗号鍵ＤＢ

Ｋｓ　選択鍵

ＭＴ　携帯端末

Ｎ　ノード

Ｎｘ　新規ノード

１００１　パケット受信部

１００２　検知部

１００３　パケット送信部

１００４　鍵受信部

１００５　設定部

１００６　抽出部

１００７　生成部

１００８　復号部

１００９　出力部

１０１０　取得部

１０１１　暗号化処理部

１２０１　受信部

１２０２　特定部

１２０３　更新部

１２０４　選択部

１２０５　送信部

請求の範囲

[請求項1] 複数のアドホックネットワークのうち通信圏内にあるアドホックネットワーク群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前記ノードの通信圏内にある各近隣ノードから、前記各アドホックネットワーク内のゲートウェイ固有の鍵を用いて暗号化された暗号化パケットを受信するパケット受信工程と、

前記パケット受信工程によって前記各近隣ノードから受信された暗号化パケット群の各々の暗号化パケットの中から前記各近隣ノードのアドレスを抽出する抽出工程と、

前記複数のアドホックネットワーク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、ノード数および前記各アドホックネットワーク内の各ノードのアドレス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、前記抽出工程によって抽出された前記各近隣ノードのアドレスを含むパケットを前記サーバに送信するパケット送信工程と、

前記パケット送信工程によって送信されたパケットから得られる前記各近隣ノードのアドレスから特定された前記各ゲートウェイが属する前記アドホックネットワーク群のうち、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、前記携帯端末を介して、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] 前記複数の暗号化パケットを、前記設定工程によって設定された鍵で復号する復号工程と、

前記復号工程による復号結果を出力する出力工程と、

を含む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] 複数のアドホックネットワークで構成されるネットワークシステムの中の各アドホックネットワーク内のゲートウェイごとにゲートウェイ固有の鍵および配下のノード数を関連付けた第１のデータベースと、前記複数のアドホックネットワーク内のノードごとに所属ゲートウェイの識別情報を関連付けた第２のデータベースと、を有し、前記各アドホックネットワークの各ゲートウェイと通信可能なサーバ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いずれのアドホックネットワーク内のゲートウェイ固有の鍵も未設定なノードに接続された携帯端末を介して、前記ノードから前記ノードのアドレスおよび前記ノードの近隣ノードのアドレスを含む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パケットに含まれている前記各近隣ノードのアドレスに基づいて、前記各近隣ノードの所属ゲートウェイを、前記第２のデータベースから特定する第１の特定工程と、

前記第１の特定工程によって特定された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、前記第１のデータベースから特定する第２の特定工程と、

前記複数のアドホックネットワークのうち、前記第２の特定工程によって特定された前記各ゲートウェイの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、前記第１のデータベースにおける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4] 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、前記第１のデータベースにおける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３に記載の鍵設定方法。

[請求項5] 前記第１の特定工程によって特定されたゲートウェイごとに前記近隣ノードのアドレス数を特定する第３の特定工程を含み、

前記選択工程は、

前記第３の特定工程によって前記ゲートウェイごとに特定された近隣ノードのアドレス数に基づいて、前記第２の特定工程によって特定された前記各ゲートウェイの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、前記第１のデータベースにおける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３に記載の鍵設定方法。

[請求項6] 前記ノードのアドレスを、前記選択工程によって選択された鍵に対応するゲートウェイの識別情報に関連付けて、前記第２のデータベースに登録する更新工程を含むことを特徴とする請求項３～５のいずれか一つに記載の鍵設定方法。

[請求項7] 複数のアドホックネットワークのうち通信圏内にあるアドホックネットワーク群からのパケットを受信可能なノードであって、

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前記ノードの通信圏内にある各近隣ノードから、前記各アドホックネットワーク内のゲートウェイ固有の鍵を用いて暗号化された暗号化パケットを受信するパケット受信手段と、

前記パケット受信手段によって前記各近隣ノードから受信された暗

号化パケット群の各々の暗号化パケットの中から前記各近隣ノードのアドレスを抽出する抽出手段と、

前記複数のアドホックネットワーク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、ノード数および前記各アドホックネットワーク内の各ノードのアドレス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、前記抽出手段によって抽出された前記各近隣ノードのアドレスを含むパケットを前記サーバに送信するパケット送信手段と、

前記パケット送信手段によって送信されたパケットから得られる前記各近隣ノードのアドレスから特定された前記各ゲートウェイが属する前記アドホックネットワーク群のうち、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8] 前記複数の暗号化パケットを、前記設定手段によって設定された鍵で復号する復号手段と、

前記復号手段による復号結果を出力する出力手段と、

を備えることを特徴とする請求項７に記載のノード。

[請求項9] 複数のアドホックネットワークで構成されるネットワークシステムの中の各アドホックネットワークの各ゲートウェイと通信可能なサーバであって、

前記各アドホックネットワーク内のゲートウェイごとにゲートウェイ固有の鍵および配下のノード数を関連付けた第１の記憶手段と、

前記複数のアドホックネットワーク内のノードごとに所属ゲートウェイの識別情報を関連付けた第２の記憶手段と、

前記複数のアドホックネットワークのいずれのアドホックネットワーク内のゲートウェイ固有の鍵も未設定なノードに接続された携帯端末を介して、前記ノードから前記ノードのアドレスおよび前記ノードの近隣ノードのアドレスを含む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パケットに含まれている前記各近隣ノードのアドレスに基づいて、前記各近隣ノードの所属ゲートウェイを、前記第２の記憶手段から特定する第１の特定処理と、前記第１の特定処理によって特定された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、前記第１の記憶手段から特定する第２の特定処理と、を実行する特定手段と、

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前記各ゲートウェイの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、前記第１の記憶手段における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10] 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、前記第１のデータベースにおける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９に記載のサーバ。

[請求項11] 前記特定手段は、

前記第１の特定処理によって特定されたゲートウェイごとに前記近

隣ノードのアドレス数を特定する第３の特定処理を実行し、

前記選択手段は、

前記特定手段によって前記ゲートウェイごとに特定された近隣ノードのアドレス数に基づいて、前記第２の特定手段によって特定された前記各ゲートウェイの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、前記第１のデータベースにおける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９に記載のサーバ。

[請求項12] 前記ノードのアドレスを、前記選択手段によって選択された鍵に対応するゲートウェイの識別情報に関連付けて、前記第２のデータベースに登録する更新手段を備えることを特徴とする請求項９～１１のいずれか一つに記載のサーバ。

[請求項13] 複数のアドホックネットワークで構成されるネットワークシステムであって、

前記ネットワークシステムの中の各アドホックネットワークの各ゲートウェイと通信可能なサーバが、

前記各アドホックネットワーク内のゲートウェイごとにゲートウェイ固有の鍵および配下のノード数を関連付けた第１の記憶手段と、

前記複数のアドホックネットワーク内のノードごとに所属ゲートウェイの識別情報を関連付けた第２の記憶手段と、

前記複数のアドホックネットワークのいずれのアドホックネットワーク内のゲートウェイ固有の鍵も未設定なノードに接続された携帯端末を介して、前記ノードから前記ノードのアドレスおよび前記ノードの近隣ノードのアドレスを含む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パケットに含まれている前記各近隣ノードのアドレスに基づいて、前記各近隣ノードの所属ゲートウェイを、前記第２の記憶手段から特定する第１の特定処理と、前記第１

の特定処理によって特定された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、前記第１の記憶手段から特定する第２の特定処理と、を実行する特定手段と、

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前記各ゲートウェイの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、前記第１の記憶手段における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、

前記ノードが、

前記複数のアドホックネットワークのうち通信圏内にある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前記ノードの通信圏内にある各近隣ノードから、前記各アドホックネットワーク内のゲートウェイ固有の鍵を用いて暗号化された暗号化パケットを受信するパケット受信手段と、

前記パケット受信手段によって前記各近隣ノードから受信された暗号化パケット群の各々の暗号化パケットの中から前記各近隣ノードのアドレスを抽出する抽出手段と、

前記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、

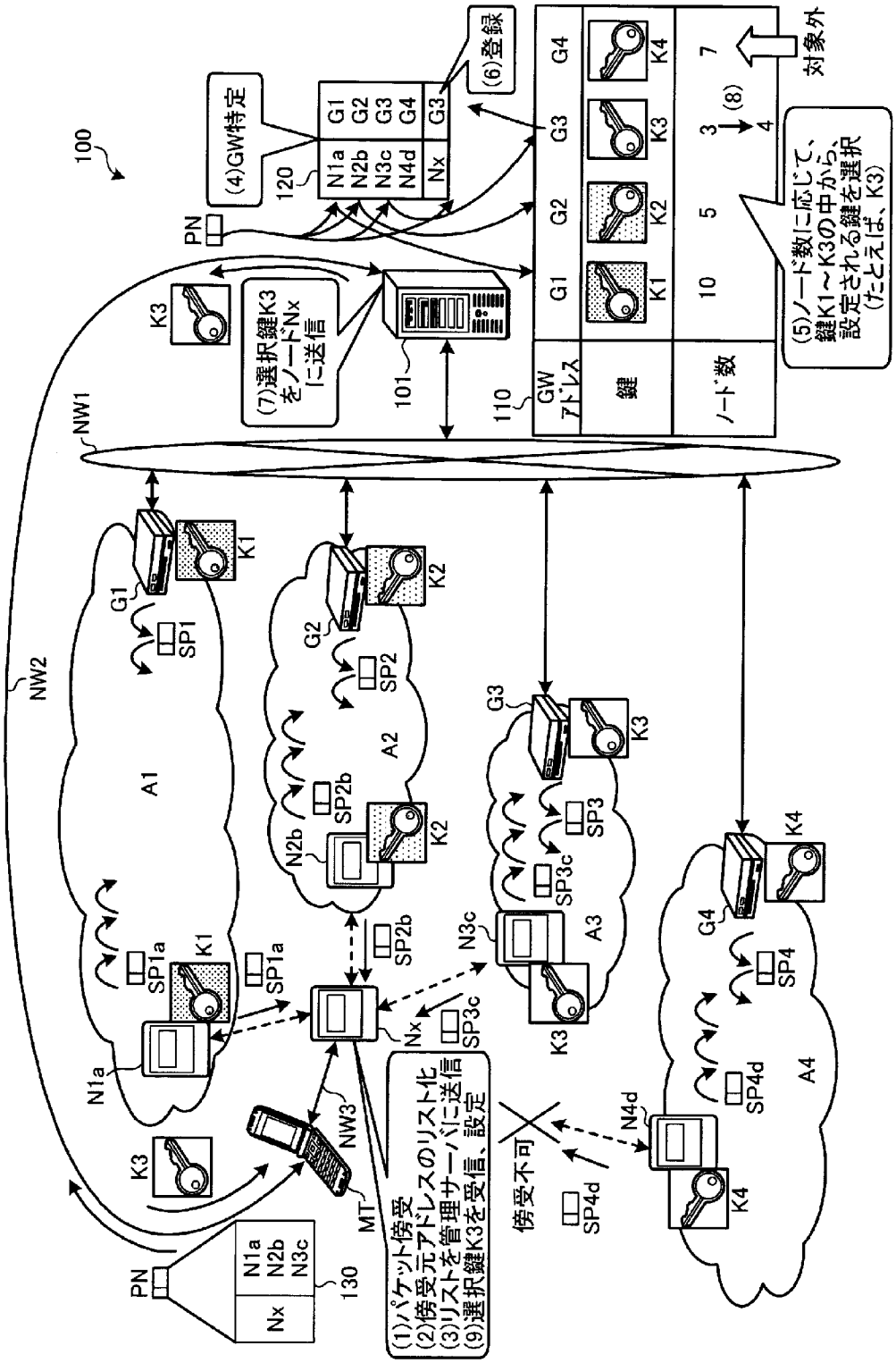
前記検知手段によって前記携帯端末との接続が検知された場合、前記携帯端末を介して、前記抽出手段によって抽出された前記各近隣ノードのアドレスを含むパケットを前記サーバに送信するパケット送信手段と、

前記パケット送信手段によって送信された結果、前記送信手段によって送信されてきた選択鍵を、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、

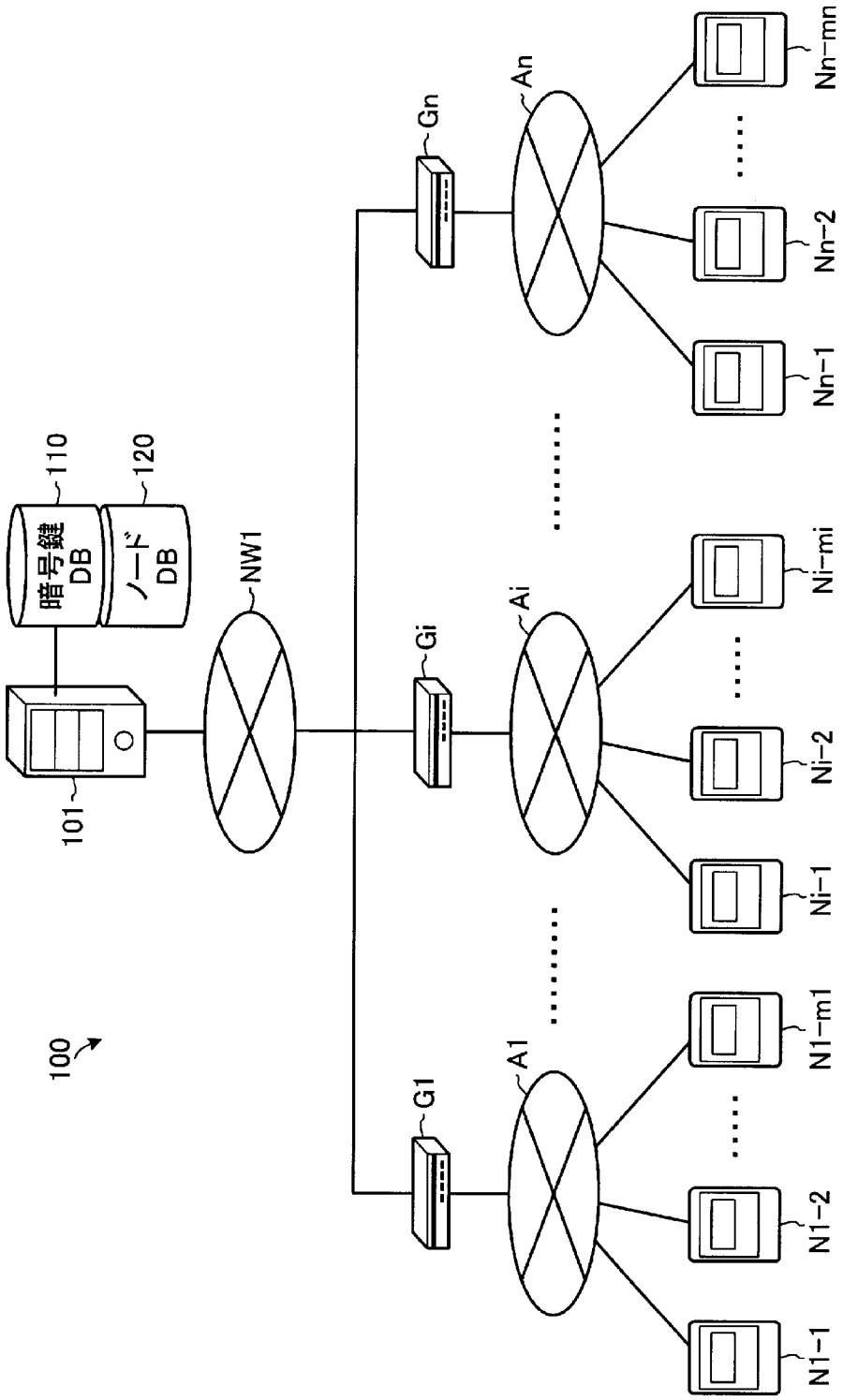
前記鍵受信手段によって受信された鍵を、前記いずれかのアドホックネットワーク内でマルチホップ通信させるパケットを暗号化するための鍵に設定する設定手段と、

を備えることを特徴とするネットワークシステム。

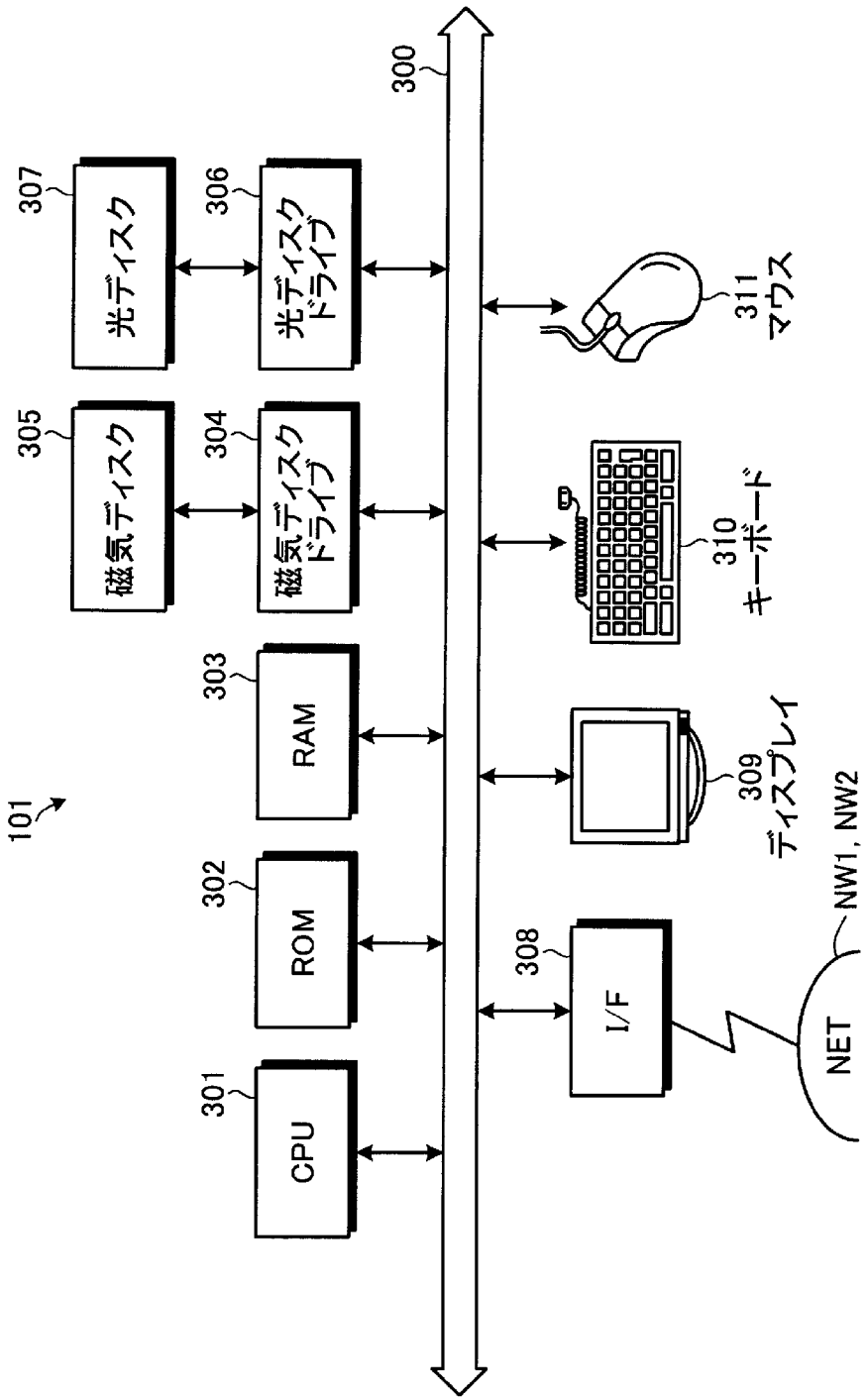
[図1]


100
NW1
NW2
NW3
A1
A2
A3
A4
G1
G2
G3
G4
K1
K2
K3
K4
SP1
SP2
SP2b
SP3
SP3c
SP4
SP4d
SP1a
N1a
N2b
N3c
Nx
N4d
MT
PN
101
110
120
130
GW アドレス
鍵
ノード数
10
5
3
4
7
(4)GW特定
(6)登録
(7)選択鍵K3をノードNxに送信
(8)
(5)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)
対象外
(1)パケット傍受
(2)傍受元アドレスのリスト化
(3)リストを管理サーバに送信
(9)選択鍵K3を受信、設定
傍受不可

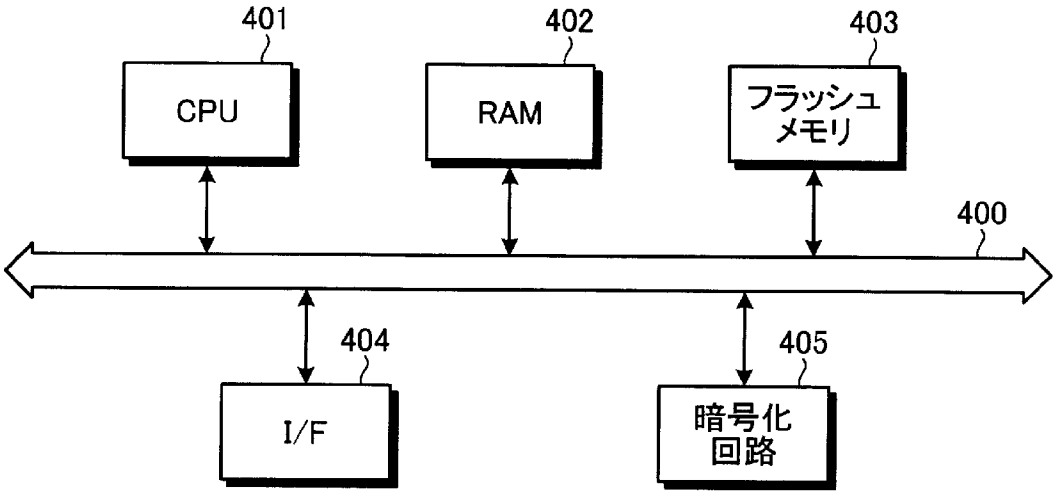
[図2]


100
101
110
暗号鍵 DB
120
ノード 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

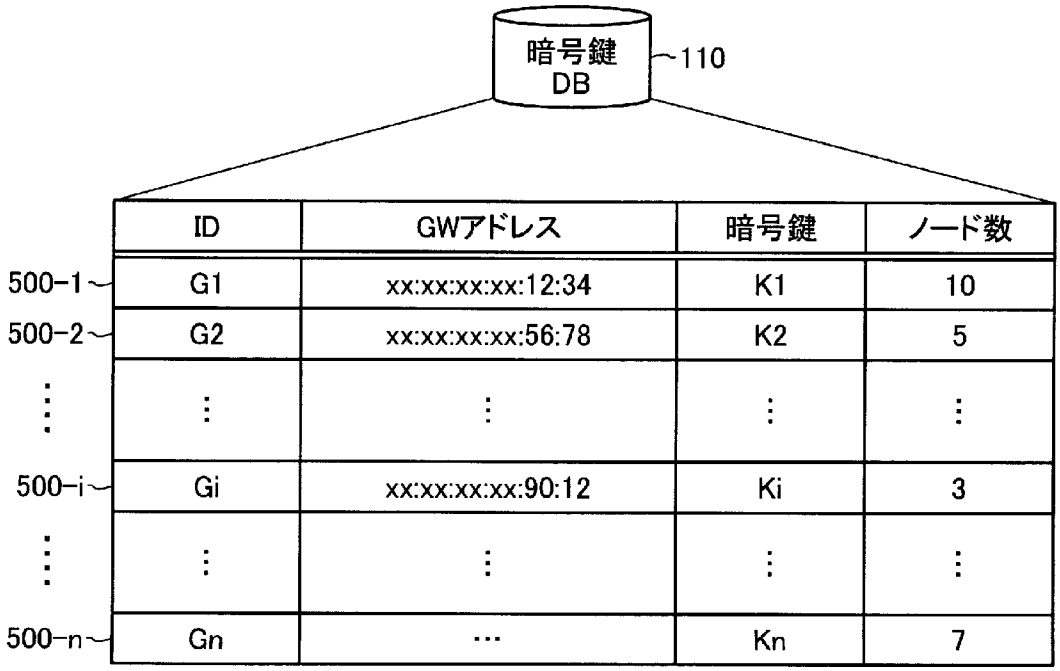
[図3]


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

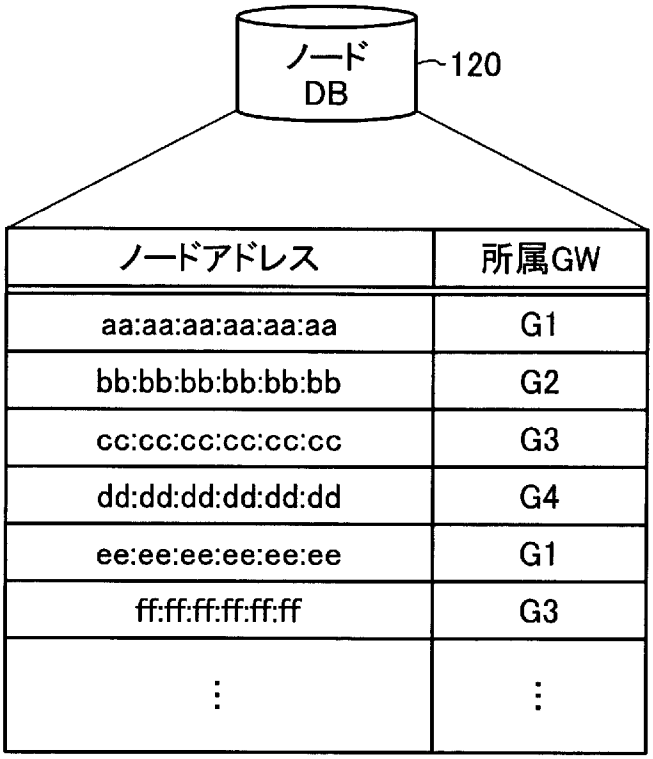
[図4]


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]

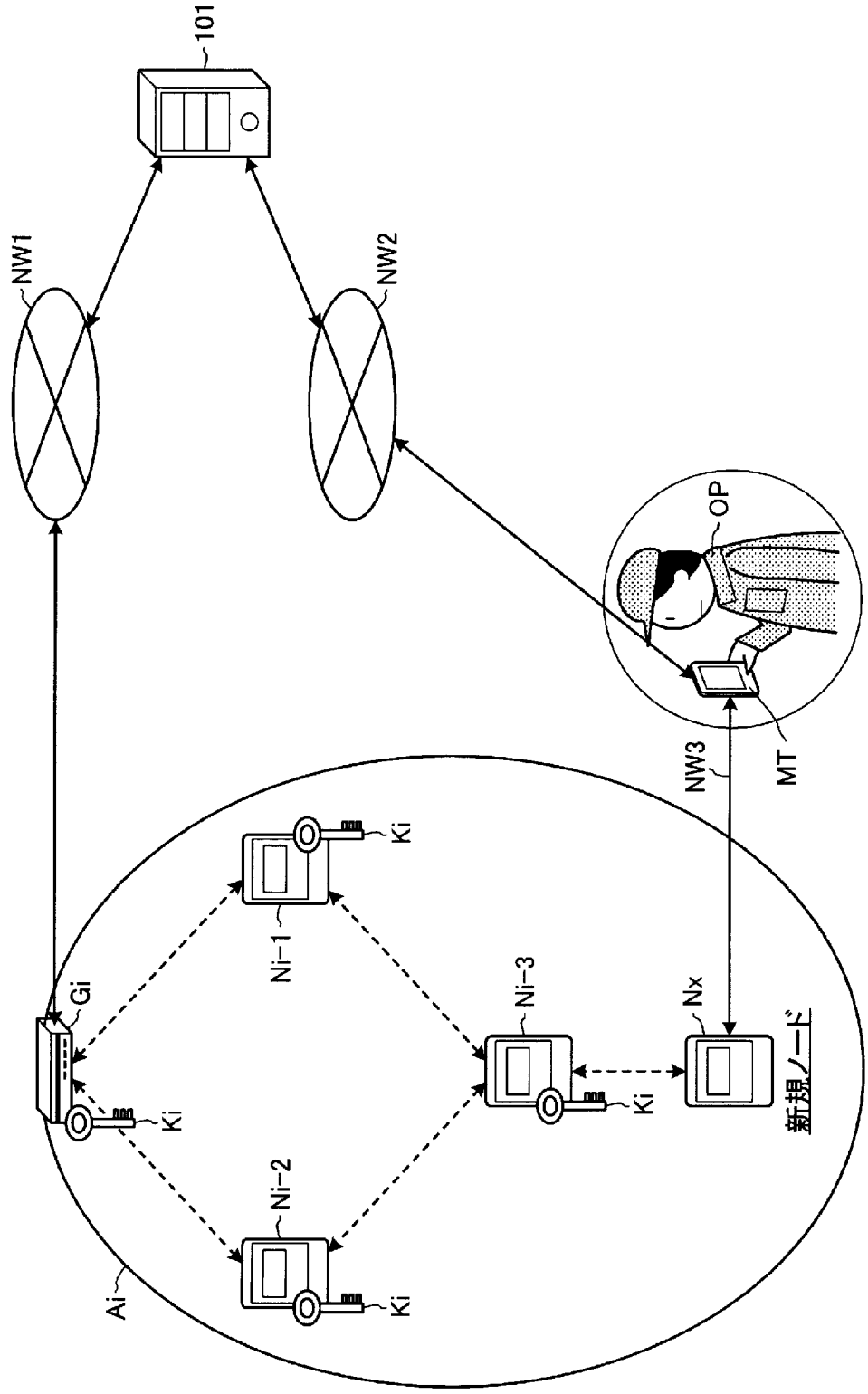

暗号鍵
DB
110
ID
GWアドレス
暗号鍵
ノード数
500-1
G1
xx:xx:xx:xx:12:34
K1
10
500-2
G2
xx:xx:xx:xx:56:78
K2
5
500-i
Gi
xx:xx:xx:xx:90:12
Ki
3
500-n
Gn
Kn
7

[図6]

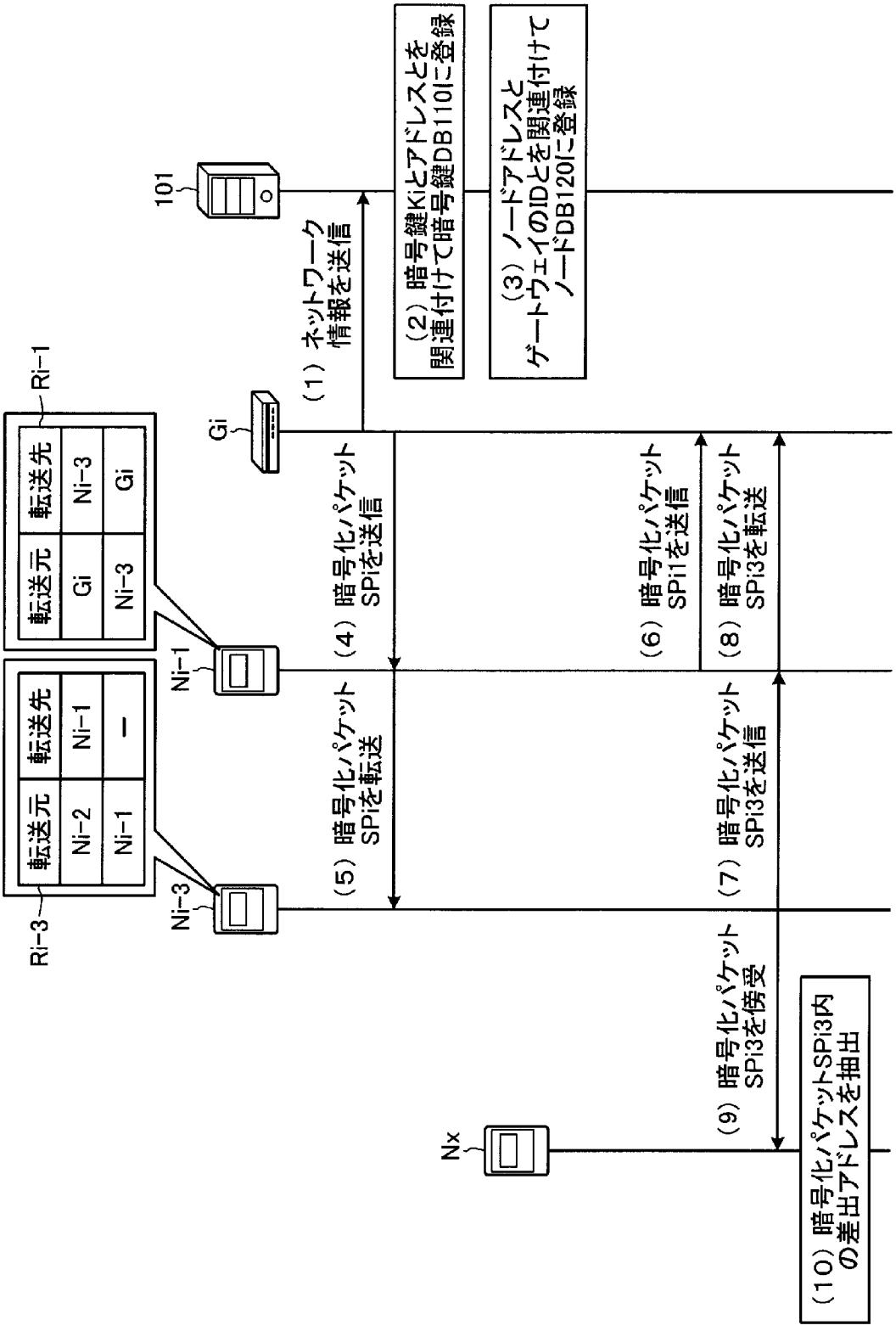


ノードアドレス	所属GW
aa:aa:aa:aa:aa:aa	G1
bb:bb:bb:bb:bb:bb	G2
cc:cc:cc:cc:cc:cc	G3
dd:dd:dd:dd:dd:dd	G4
ee:ee:ee:ee:ee:ee	G1
ff:ff:ff:ff:ff:ff	G3
⋮	⋮

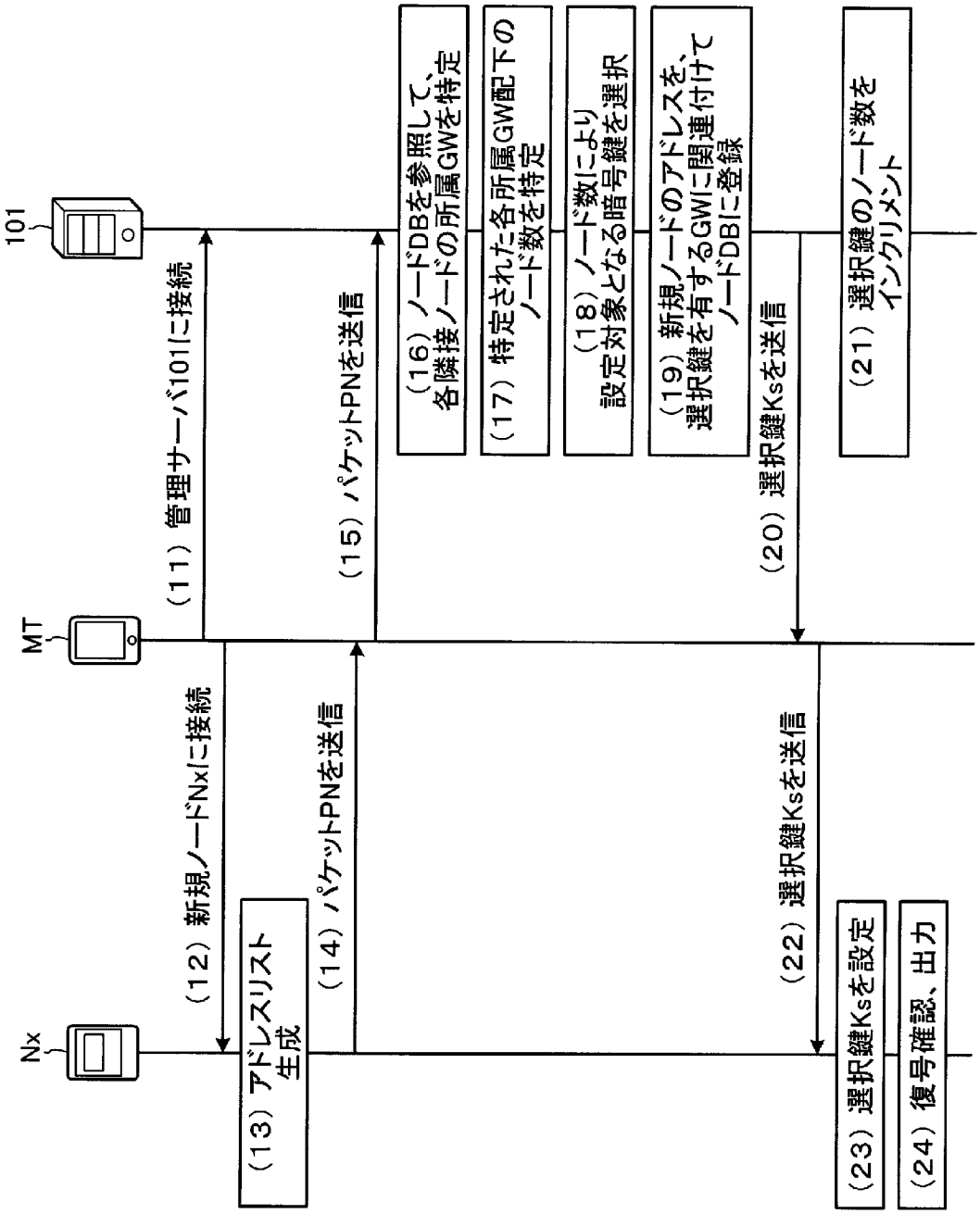
[図7]



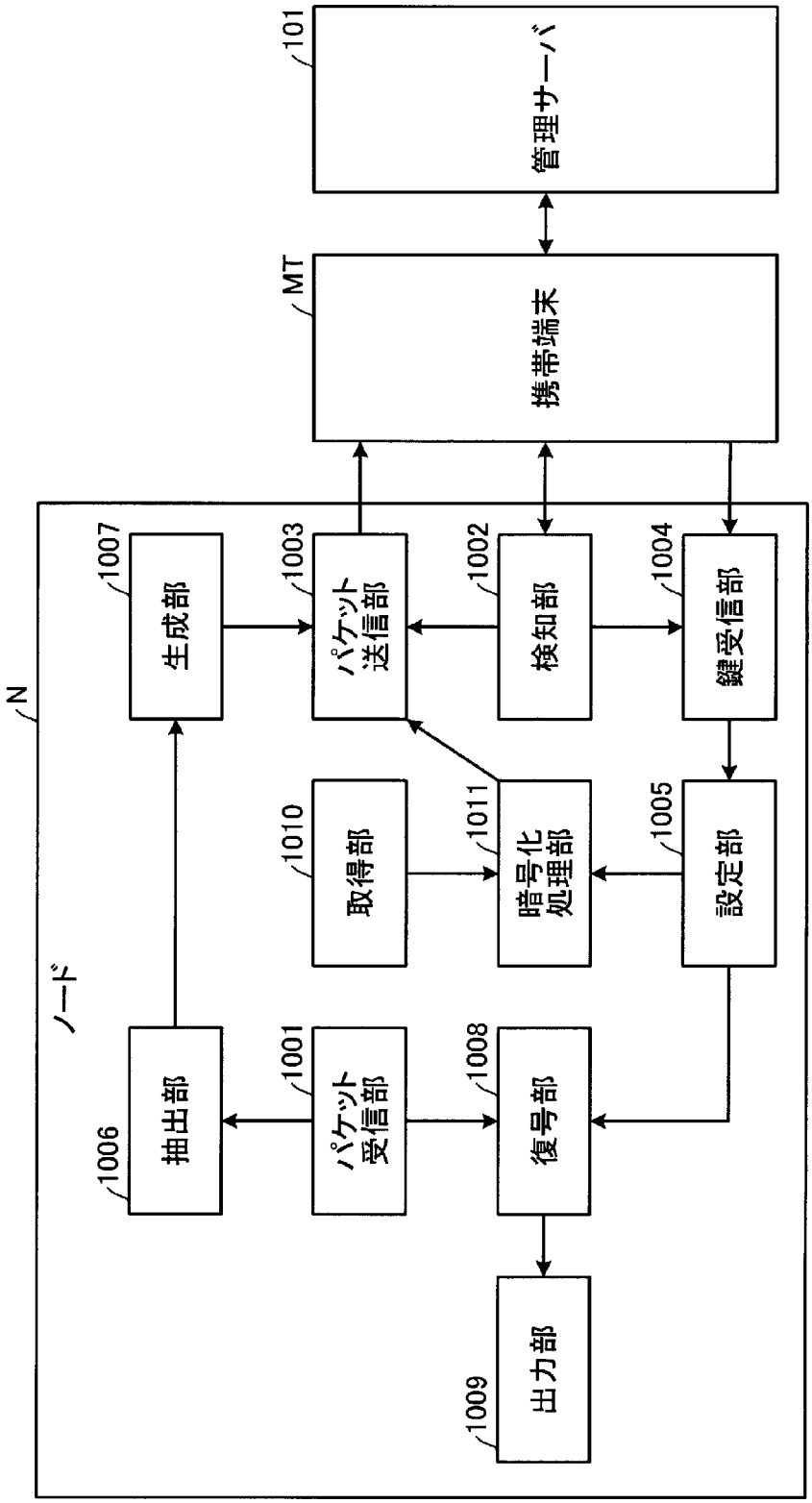
[図8]


101
Gi
Ni-1
Ni-3
Nx
Ri-1
転送元
転送先
Gi
Ni-3
Ni-3
Gi
Ri-3
転送元
転送先
Ni-2
Ni-1
Ni-1
—
(1) ネットワーク情報を送信
(2) 暗号鍵Kiとアドレスとを関連付けて暗号鍵DB110Iに登録
(3) ノードアドレスとゲートウェイのIDとを関連付けてノードDB120Iに登録
(4) 暗号化パケットSPiを送信
(5) 暗号化パケットSPiを転送
(6) 暗号化パケットSPi1を送信
(7) 暗号化パケットSPi3を送信
(8) 暗号化パケットSPi3を転送
(9) 暗号化パケットSPi3を傍受
(10) 暗号化パケットSPi3内の差出アドレスを抽出

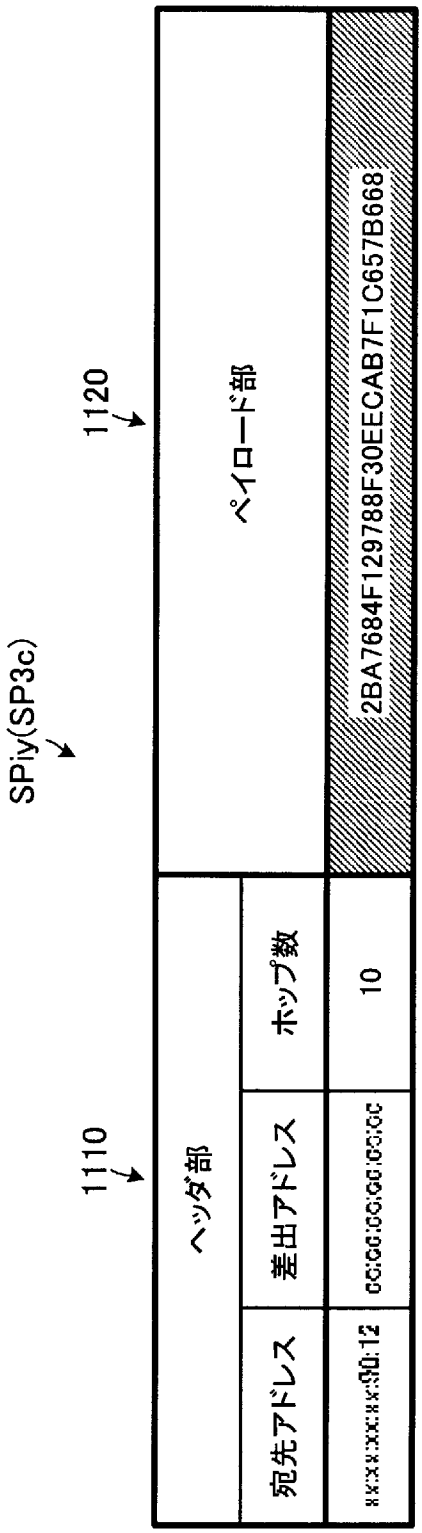
[図9]


101
MT
Nx
(11) 管理サーバ101に接続
(12) 新規ノードNxに接続
(13) アドレスリスト生成
(14) パケットPNを送信
(15) パケットPNを送信
(16) ノードDBを参照して、各隣接ノードの所属GWを特定
(17) 特定された各所属GW配下のノード数を特定
(18) ノード数により設定対象となる暗号鍵を選択
(19) 新規ノードのアドレスを、選択鍵を有するGWに関連付けてノードDBに登録
(20) 選択鍵Ksを送信
(21) 選択鍵のノード数をインクリメント
(22) 選択鍵Ksを送信
(23) 選択鍵Ksを設定
(24) 復号確認、出力

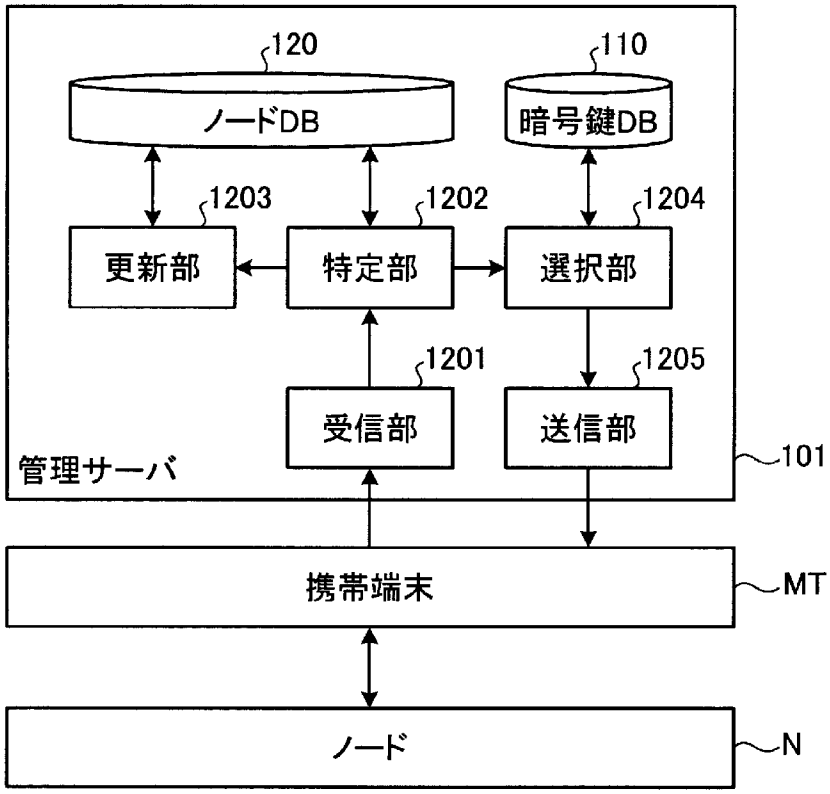
[図10]


101
管理サーバ
MT
携帯端末
N
ノード
1007
生成部
1003
パケット送信部
1002
検知部
1004
鍵受信部
1010
取得部
1011
暗号化処理部
1005
設定部
1006
抽出部
1001
パケット受信部
1008
復号部
1009
出力部

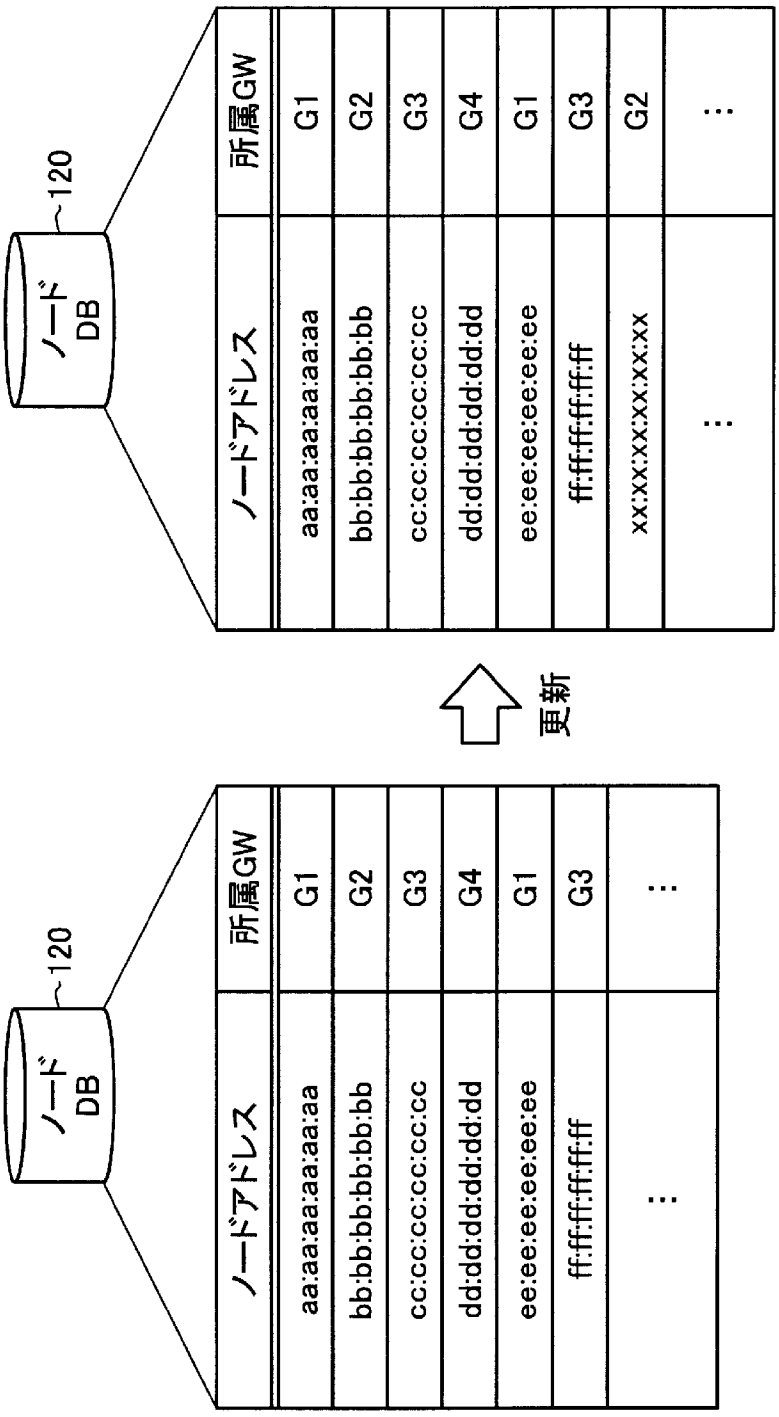
[図11]


SPiy(SP3c)
1110
1120
ヘッダ部
宛先アドレス
差出アドレス
ホップ数
10
ペイロード部
2BA7684F129788F30EECAB7F1C657B668

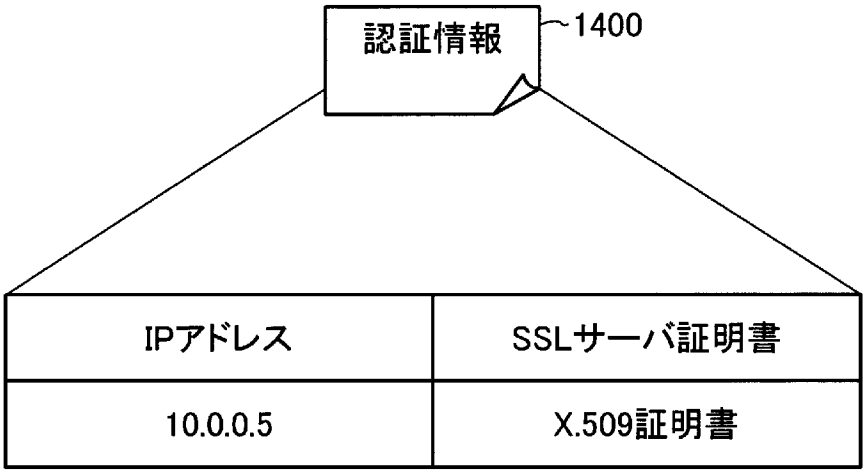
[図12]


120
ノードDB
110
暗号鍵DB
1203
1202
1204
更新部
特定部
選択部
1201
1205
受信部
送信部
管理サーバ
101
携帯端末
MT
ノード
N

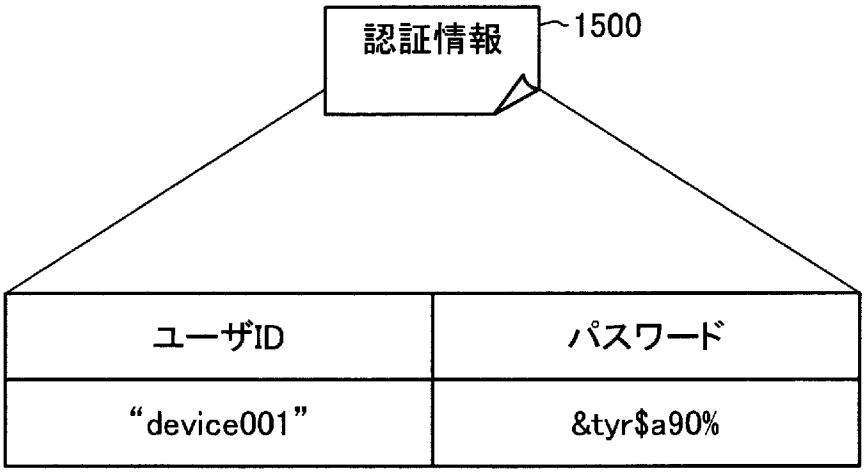
[図13]


120
ノードDB
ノードアドレス
所属GW
aa:aa:aa:aa:aa:aa
G1
bb:bb:bb:bb:bb:bb
G2
cc:cc:cc:cc:cc:cc
G3
dd:dd:dd:dd:dd:dd
G4
ee:ee:ee:ee:ee:ee
G1
ff:ff:ff:ff:ff:ff
G3
xx:xx:xx:xx:xx:xx
G2
更新
120
ノードDB
ノードアドレス
所属GW
aa:aa:aa:aa:aa:aa
G1
bb:bb:bb:bb:bb:bb
G2
cc:cc:cc:cc:cc:cc
G3
dd:dd:dd:dd:dd:dd
G4
ee:ee:ee:ee:ee:ee
G1
ff:ff:ff:ff:ff:ff
G3

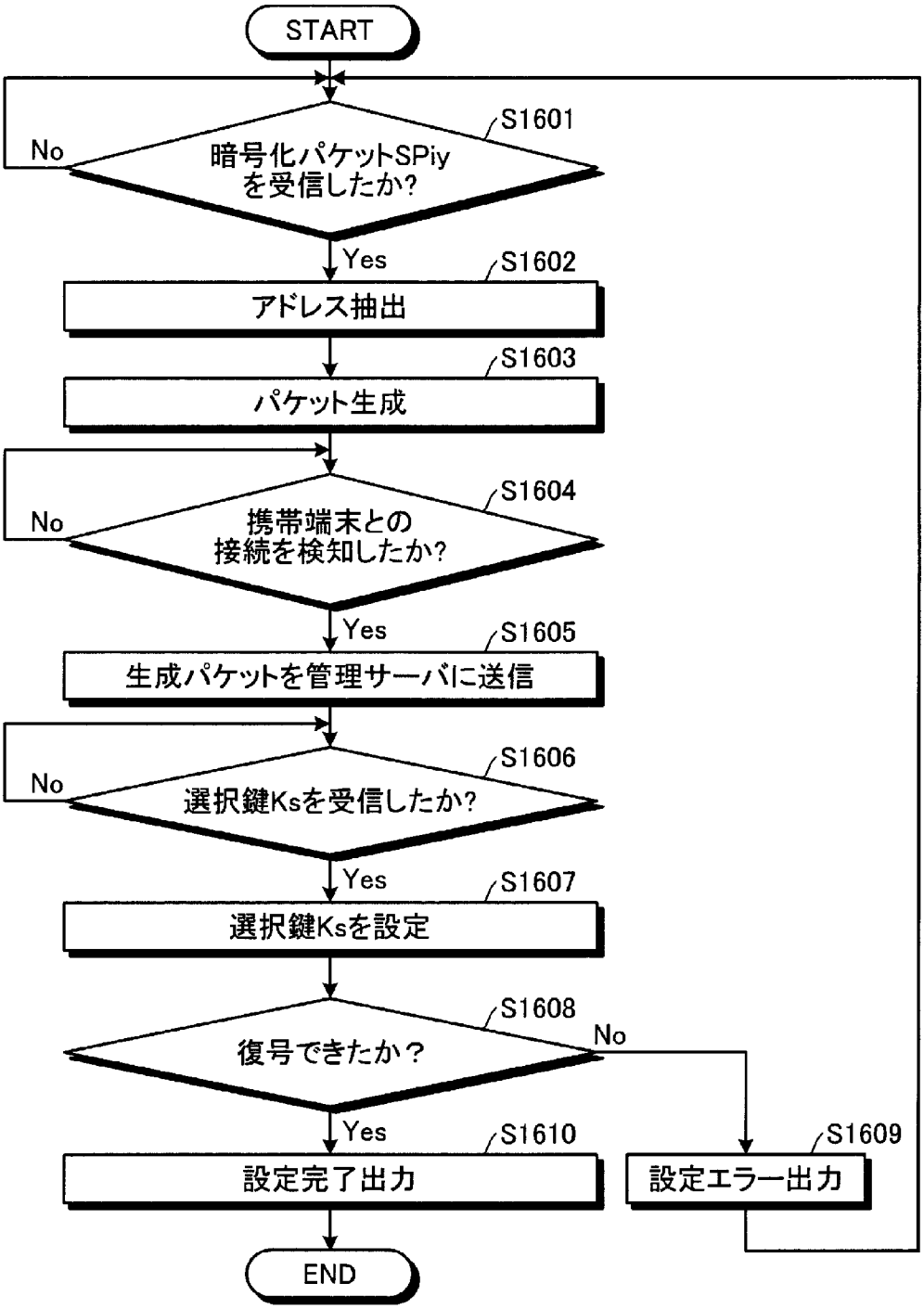
[図14]


認証情報
1400
IPアドレス
SSLサーバ証明書
10.0.0.5
X.509証明書

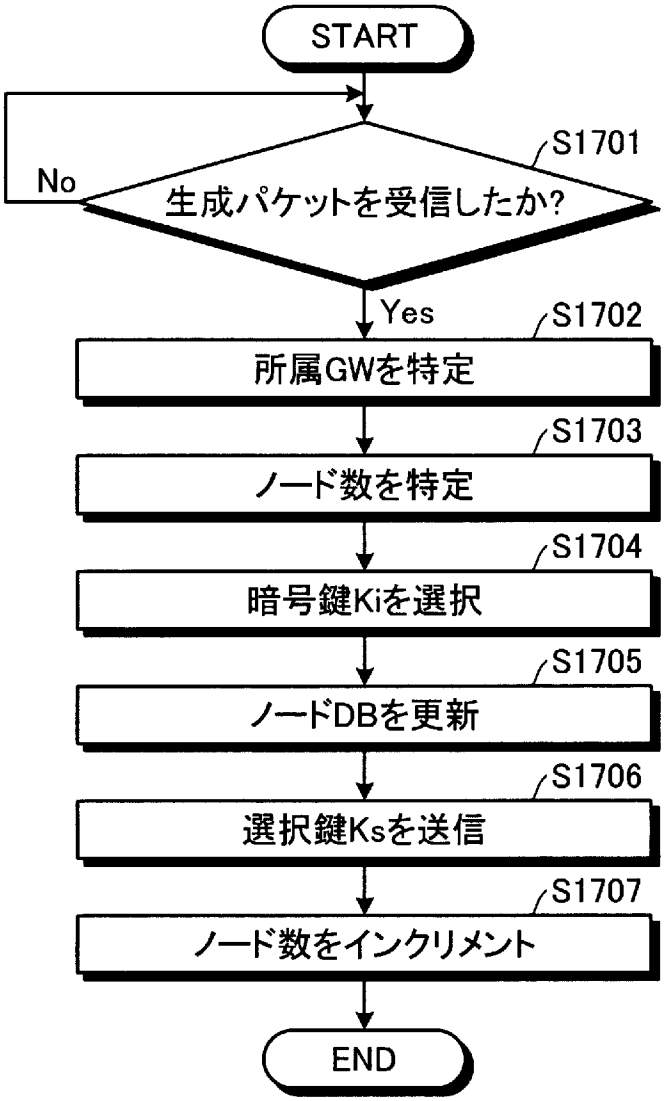
[図15]


認証情報
1500
ユーザID
パスワード
“device001”
&tyr$a90%

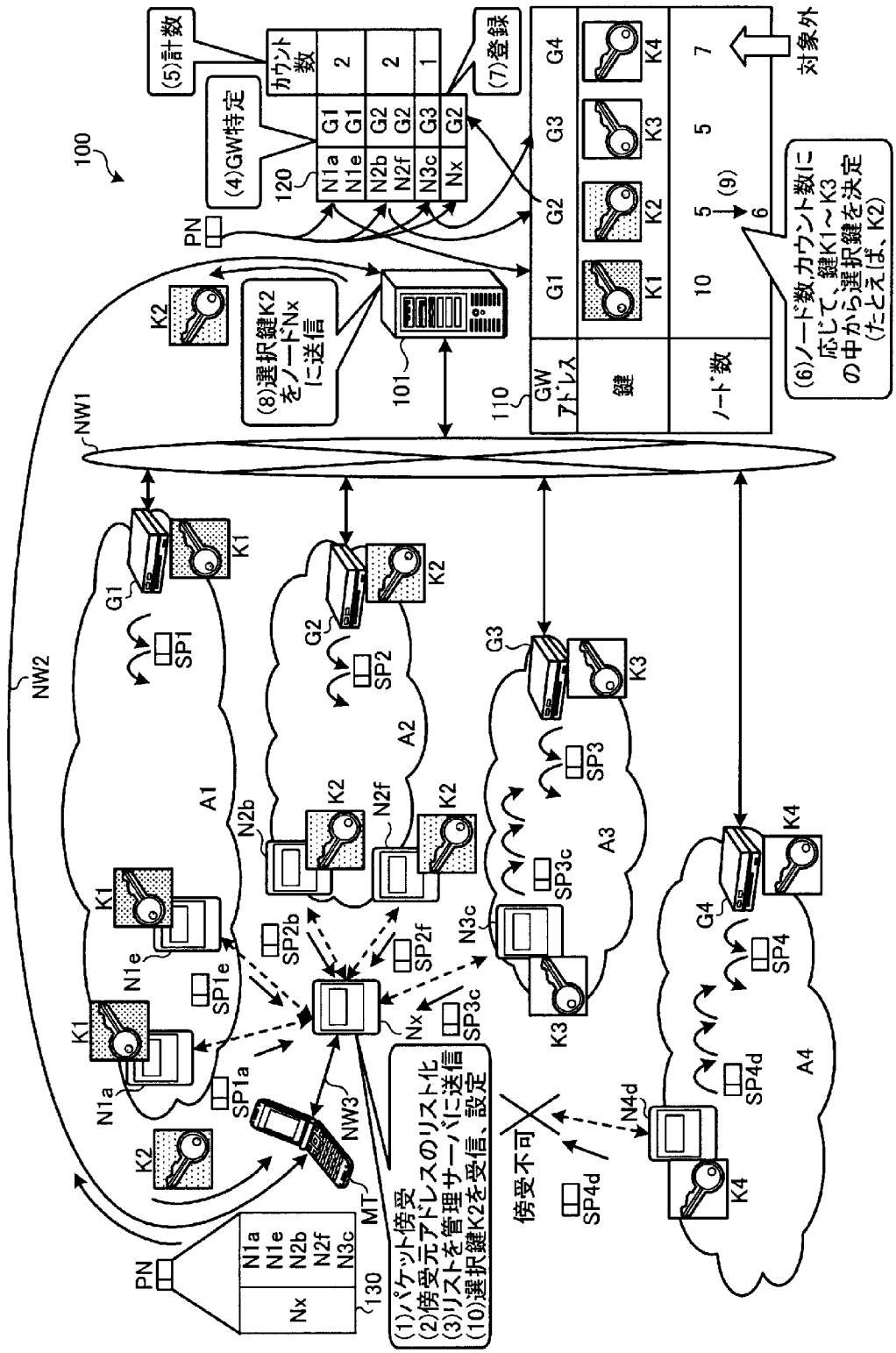
[図16]


START
S1601
No
暗号化パケットSPiy
を受信したか?
Yes
S1602
アドレス抽出
S1603
パケット生成
S1604
No
携帯端末との
接続を検知したか?
Yes
S1605
生成パケットを管理サーバに送信
S1606
No
選択鍵Ksを受信したか?
Yes
S1607
選択鍵Ksを設定
S1608
復号できたか?
No
Yes
S1610
設定完了出力
S1609
設定エラー出力
END

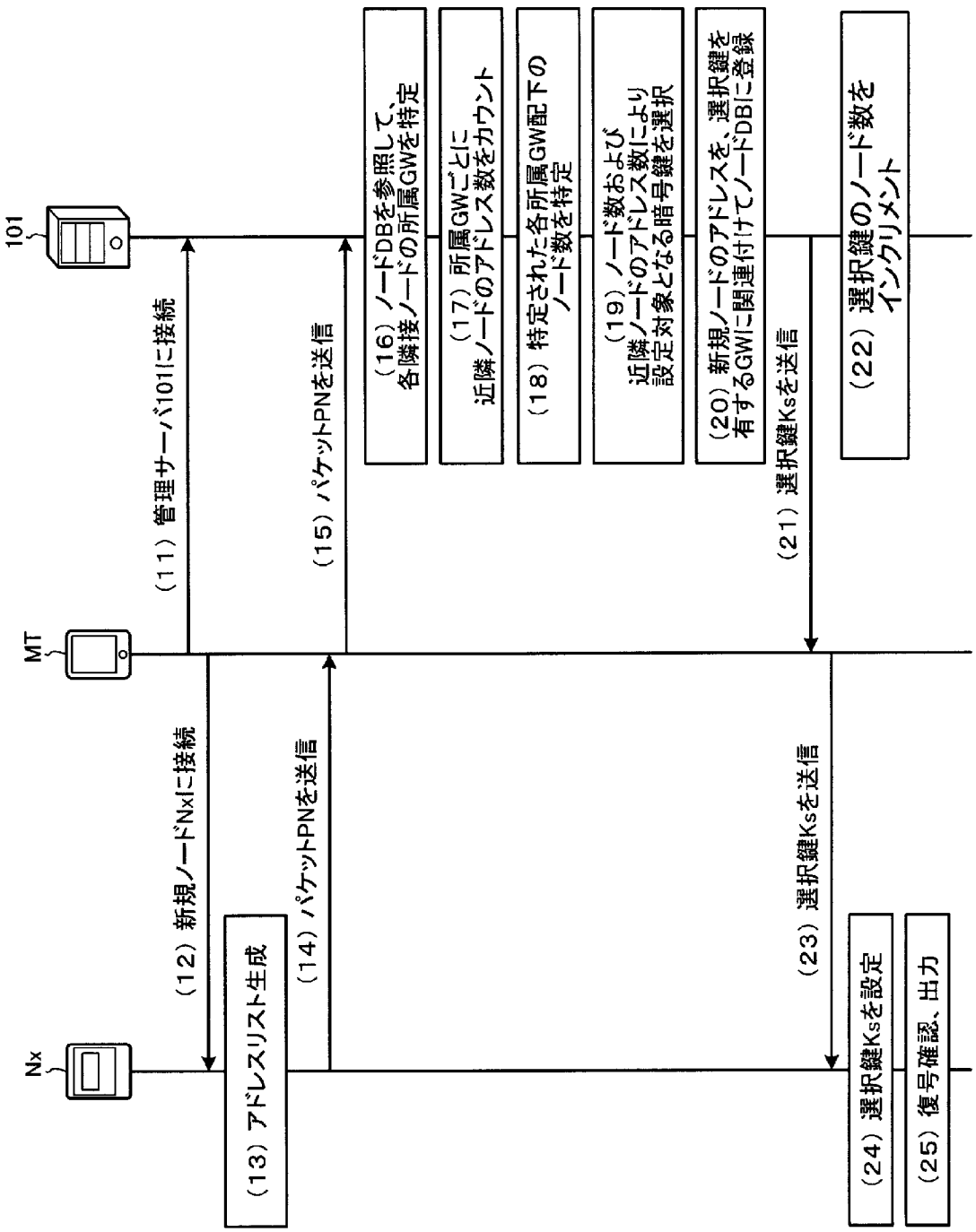
[図17]


START
S1701
No
生成パケットを受信したか?
Yes
S1702
所属GWを特定
S1703
ノード数を特定
S1704
暗号鍵Kiを選択
S1705
ノードDBを更新
S1706
選択鍵Ksを送信
S1707
ノード数をインクリメント
END

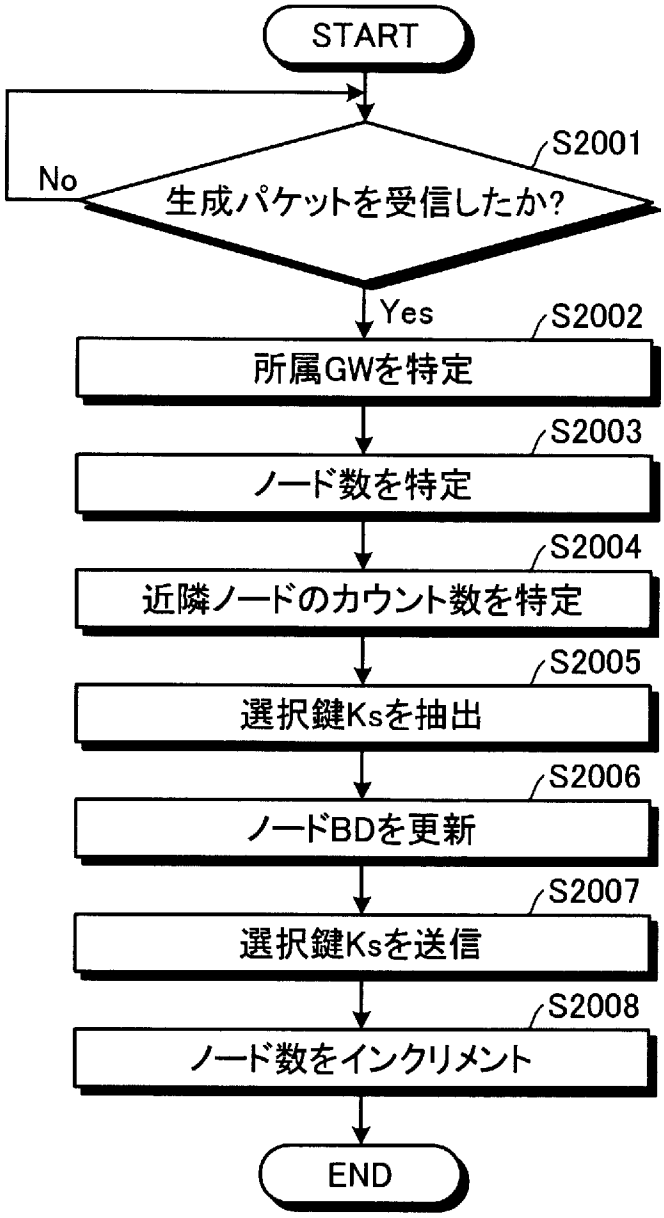
[図18]


100
(5)計数
(4)GW特定
(7)登録
カウント数
120
N1a G1 2
N1e G1
N2b G2 2
N2f G2
N3c G3 1
Nx G2
PN
K2
(8)選択鍵K2をノードNxに送信
101
110
GWアドレス
鍵
ノード数
G1 G2 G3 G4
K1 K2 K3 K4
10 5 5 7
(9)
6
対象外
(6)ノード数,カウント数に応じて、鍵K1～K3の中から選択鍵を決定(たとえば、K2)
NW1
NW2
NW3
A1
A2
A3
A4
SP1
SP1a
SP1e
SP2
SP2b
SP2f
SP3
SP3c
SP4
SP4d
N1a
N1e
N2b
N2f
N3c
N4d
Nx
MT
130
(1)パケット傍受
(2)傍受元アドレスのリスト化
(3)リストを管理サーバに送信
(10)選択鍵K2を受信、設定
傍受不可

[図19]


101
MT
Nx
(11) 管理サーバ101に接続
(12) 新規ノードNxに接続
(13) アドレスリスト生成
(14) パケットPNを送信
(15) パケットPNを送信
(16) ノードDBを参照して、各隣接ノードの所属GWを特定
(17) 所属GWごとに近隣ノードのアドレス数をカウント
(18) 特定された各所属GW配下のノード数を特定
(19) ノード数および近隣ノードのアドレス数により設定対象となる暗号鍵を選択
(20) 新規ノードのアドレスを、選択鍵を有するGWに関連付けてノードDBに登録
(21) 選択鍵Ksを送信
(22) 選択鍵のノード数をインクリメント
(23) 選択鍵Ksを送信
(24) 選択鍵Ksを設定
(25) 復号確認、出力

[図20]


START
S2001
No
生成パケットを受信したか?
Yes
S2002
所属GWを特定
S2003
ノード数を特定
S2004
近隣ノードのカウント数を特定
S2005
選択鍵Ksを抽出
S2006
ノードBDを更新
S2007
選択鍵Ksを送信
S2008
ノード数をインクリメント
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/051963

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	1-13
A	JP 2007-74393 A (NTT Docomo Inc.), 22 March 2007 (22.03.2007), entire text; all drawings (Family: none)	1-13
A	JP 2007-116319 A (Saxa, Inc.), 10 May 2007 (10.05.2007), entire text; all drawings (Family: none)	1-13

☒ 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	Date of mailing of the international search report
25 February, 2011 (25.02.11)	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/JP2011/051963

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 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	1-13
A	JP 2009-71707 A (Oki Electric Industry Co., Ltd.), 02 April 2009 (02.04.2009), entire text; all drawings (Family: none)	1-13

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０５１９６３

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	1-13
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)	1-13

☑　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	国際調査報告の発送日
２５．０２．２０１１	０８．０３．２０１１

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ	４５３８
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	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 2007-116319 A (サクサ株式会社) 2007.05.10, 全文、全図 (ファミリーなし)	1-13
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	1-13
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)	1-13