(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5775963号
(P5775963)

(45)発行日　平成27年9月9日(2015.9.9)　(24)登録日　平成27年7月10日(2015.7.10)

(51)Int.Cl.　F I

H04L 9/08	(2006.01)	H04L	9/00	601C
H04L 9/14	(2006.01)	H04L	9/00	641

請求項の数 6　(全 20 頁)

(21)出願番号　特願2014-505782 (P2014-505782)
(86)(22)出願日　平成23年6月9日 (2011.6.9)
(65)公表番号　特表2014-513895 (P2014-513895A)
(43)公表日　平成26年6月5日 (2014.6.5)
(86)国際出願番号　PCT/IN2011/000385
(87)国際公開番号　WO2012/143931
(87)国際公開日　平成24年10月26日 (2012.10.26)
審査請求日　平成25年11月21日 (2013.11.21)
(31)優先権主張番号　1283/MUM/2011
(32)優先日　平成23年4月21日 (2011.4.21)
(33)優先権主張国　インド(IN)

(73)特許権者　510337621
タタ　コンサルタンシー　サービシズ　リミテッド
TATA Consultancy Services Limited
インド国　マハーラシュトラ、ムンバイ　４０００２１、ナリマン　ポイント、ナーマル　ビルディング　９階
Nirmal Building, 9th Floor, Nariman Point, Mumbai 400021, Maharashtra, India.
(74)代理人　100130111
弁理士　新保　斉

最終頁に続く

(54)【発明の名称】無線センサネットワークにおいてデータ集約中にプライバシーを保全する方法及びシステム

(57)【特許請求の範囲】

【請求項１】

非階層無線ネットワークで安全にデータを集約する方法であって、前記ネットワークにおいて、ネットワークのセンサノード間にピアツーピア通信が存在しない場合であっても、拡張性が高く計算が複雑ではない自己適応型クラスタ形成を特徴とし、

ａ）前記ネットワークの第１のセットのノードをグループ化して、少なくとも１つのクラスタを形成するステップであって、前記クラスタは第１のセットのノードから４つまたは５つのノードを備え、第２のセットのノードをサーバ／アグリゲータノードによって形成するステップと、

ｂ）前記第２のセットのノードを前記クラスタから選択し、それらをグループ化して、２つのフレンド対を形成するステップであって、各対は２つまたは３つのノードをサーバ／アグリゲータノードによって前記第２のセットのノードから備えるステップと、

ｂ－２）サーバ／アグリゲータノードによってシンク／センサノードに「ハロー」メッセージを送り、それを受信したシンク／センサノードが応答失敗する場合には、そのノードはサーバ／アグリゲータノードによってパッシブまたはデッドノードとみなされ、サーバ／アグリゲータノードによってフレンド対形成の再グループ化を行うことで、シンク／センサノードの状態を監視するステップと、

ｃ）前記ネットワークの第１のセットのノード間の第１のセットの鍵のために生成された、対応する識別情報を備える前記第１のセットの鍵をサーバ／アグリゲータノードによってランダムに配布するステップと、

ｄ）前記第１のセットのノードで利用可能な前記第１のセットの鍵をサーバノードと共有するステップであって、前記サーバノードを介して前記ネットワークの前記第１のセットのノードの個々のノード間の安全な通信をシンク／センサノードによって可能にするステップと、

ｅ）前記ネットワークの前記第１のセットのノード間の鍵であり、第２のセットの鍵のために生成された、対応する識別情報を備える前記第２のセットの鍵をサーバ／アグリゲータノードによってランダムに配布するステップと、

ｆ）前記第１のセットのノードで利用可能な前記第２のセットの鍵を前記サーバノードと共有するステップであって、前記ネットワークの前記第１のセットのノードの各個々のノードと、前記サーバノードとの安全な通信をシンク／センサノードによって可能にするステップと、

ｇ）前記ネットワークの前記第１のセットのノードからの少なくとも１つの個々のノードと、前記サーバノードとの間の通信を、少なくとも１つの共有鍵をシンク／センサノードによって前記第２のセットの鍵からランダムに選択することによって確立するステップと、

ｈ）前記サーバノードを介する、前記ネットワークの前記第１のセットのノードからの少なくとも２つの個々のノード間の通信を、少なくとも１つの共有鍵をシンク／センサノードによって前記第１のセットの鍵からランダムに選択することによって確立するステップと、を備える

ことを特徴とする方法。

【請求項２】

前記サーバノードは、前記ネットワークの第１のセットのノードによって収集されるデータを集約することに関与する

請求項１に記載の方法。

【請求項３】

配布される前記第１及び第２のセットの鍵は、第３のセットの鍵のプールから生成される

請求項１に記載の方法。

【請求項４】

Ｎ／４個のクラスタは前記ネットワークで形成され、Ｎ／４が整数値の場合は、Ｎは前記ネットワーク内のノードの数を表し、各クラスタは４つのノードを含み、

前記ネットワークに形成される前記Ｎ／４個のクラスタのうちの少なくとも３つのクラスタは、Ｎ／４が整数値ではない場合は、５つのノードを含む

請求項１に記載の方法。

【請求項５】

非階層無線ネットワークで安全にデータを集約するシステムであって、前記ネットワークにおいて、ネットワークのセンサノード間にピアツーピア通信が存在しない場合であっても、拡張性が高く計算が複雑ではない自己適応型クラスタ形成を特徴とし、前記システムは、前記ネットワークのサーバノードと通信する第１のセットのノードと、前記第１のセットのノードによって収集される前記データを集約することに関与する前記サーバノードと、それに備わるプロセッサと、前記プロセッサに接続するメモリとを備え、前記プロセッサによって実行されるときに、前記プロセッサに、

ａ）前記ネットワークの第１のセットのノードを少なくとも１つのクラスタにグループ化し、前記クラスタは前記第１のセットのノードから４つまたは５つのノードを備え、サーバ／アグリゲータノードによって第２のセットのノードを形成することと、

ｂ）前記第２のセットのノードを前記クラスタから選択し、それらをグループ化して、２つのフレンド対を形成し、各対は前記第２のセットのノードから２つまたは３つのノードをサーバ／アグリゲータノードによって備えることと、

ｂ－２）サーバ／アグリゲータノードによってシンク／センサノードに「ハロー」メッセージを送り、それを受信したシンク／センサノードが応答失敗する場合には、そのノー

ドはサーバ／アグリゲータノードによってパッシブまたはデッドノードとみなされ、サーバ／アグリゲータノードによってフレンド対形成の再グループ化を行うことで、シンク／センサノードの状態を監視することと、

ｃ）前記ネットワークの第１のセットのノード間の第１のセットの鍵のために生成された、対応する識別情報を備える前記第１のセットの鍵をサーバ／アグリゲータノードによってランダムに配布することと、

ｄ）前記第１のセットのノードで利用可能な前記第１のセットの鍵をサーバノードと共有し、前記サーバノードを介して前記ネットワークの前記第１のセットのノードの個々のノード間の安全な通信をシンク／センサノードによって可能にすることと、

ｅ）前記ネットワークの前記第１のセットのノード間の鍵であり、第２のセットの鍵のために生成された、対応する識別情報を備える前記第２のセットの鍵をサーバ／アグリゲータノードによってランダムに配布することと、

ｆ）前記第１のセットのノードで利用可能な前記第２のセットの鍵を前記サーバノードと共有し、前記ネットワークの前記第１のセットのノードの各個々のノードと、前記サーバノードとの安全な通信をシンク／センサノードによって可能にすることと、

ｇ）前記ネットワークの前記第１のセットのノードからの少なくとも１つの個々のノードと、前記サーバノードとの間の通信を、少なくとも１つの共有鍵をシンク／センサノードによって前記第２のセットの鍵からランダムに選択することによって確立することと、

ｈ）前記サーバノードを介する、前記ネットワークの前記第１のセットのノードからの少なくとも２つの個々のノード間の通信を、少なくとも１つの共有鍵をシンク／センサノードによって前記第１のセットの鍵からランダムに選択することによって確立することと、を行わせる指示をする

ことを特徴とするシステム。

【請求項６】

Ｎ／４個のクラスタは前記ネットワークで形成され、Ｎ／４が整数値の場合は、Ｎは前記ネットワークのノードの数を表し、各クラスタは４つのノードを含み、

前記ネットワークに形成される前記Ｎ／４個のクラスタのうちの少なくとも３つのクラスタは、Ｎ／４が整数値ではない場合は、５つのノードを含む

請求項５に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は一般に、フラットな無線センサネットワークでのデータ集約分野に関する。具体的には、本発明は、シングルホップ非階層無線センサネットワークで様々なセンサノードによって収集されるデータを集約中に、プライバシーを保全するための方法及びシステムに関する。

【背景技術】

【０００２】

無線センサネットワーク（ＷＳＮ）は、住宅の安全性の追跡、車両の追跡、野生動物の追跡及び環境監視などの様々な用途において現在使用されている。このように、無線センサネットワークは世界中で普及しており、事務所、家庭及び敵対地域を含む様々な環境で、配備されてきた。

【０００３】

プライバシーは、インターネット及び携帯技術が極限まで浸透している現代の状況において、重要な問題である。最近では、大規模なデータ収集及び統合努力によって、プライバシーに対する懸念が増加してきた。無線センサネットワークでは、データ集約中に、サーバノードまたはデータアグリゲータノードは、特定の区域において追跡データを収集することに関与する、個々のセンサノードのデータの私有内容を探すことができる場合もある。さらに、無線リンクは、私有データを暴露するために攻撃者によって盗聴されることもある。

【０００４】
したがって、データ集約中に、各センサノードのデータがそれ自体に知られるように、センサノードでのデータのプライバシーを確実に保全することが必要となる。それによって、サーバノードのタスクは、データ集約操作を実行して、集約したデータのみをさらに処理すること、センサノードでのデータの私有内容を暴露しないようにすることにのみ制限されるべきである。さらに、攻撃者による無線リンクの盗聴も避けなければならない。
【０００５】
無線センサネットワークにおいてデータを集約する間に、センサノードの私有データを保全するための努力が過去に行われてきた。下記に既知である従来技術の一部を挙げる。
【０００６】
非特許文献１の論文は、無線センサネットワークでデータを安全に集約するために、ピアツーピアネットワークにおけるクラスタ形成を教示する、クラスタに基づく私有データ集約（ＣＰＤＡ）方式を開示する。
【０００７】
非特許文献２の論文は、クラスタ化のためにデータを共有するときに、根底となる属性値を保護する問題を是正するために、回転に基づく変換（ＲＢＴ）と呼ばれる空間データ変換方法を開示する。
【０００８】
Ｈｕａｎｇ、Ｓｈｉｈ－Ｉらによる特許文献１は、単純な対象鍵暗号アルゴリズムに基づく安全なデータ集約のための方法及びシステムを開示する。
【０００９】
Ｈｕａｎｇ、Ｓｈｉｈ－Ｉらによる特許文献２は、私有対称鍵アルゴリズムを採用することによって、階層ネットワークのプライバシー保全方式の方法及びシステムを開示する。
【００１０】
Ｇｉｒａｏらによる特許文献３は、無線センサネットワークでデータを集約する方法及びシステムを開示する。この方法及びシステムは、低エネルギー適応クラスタリング階層（ＬＥＡＣＨ）プロトコルを用いてデータを集約するためのデータアグリゲータを選択し、データ暗号化のための暗号化鍵のマルチホップ配布を可能とする。
【００１１】
Ｓｕｎ、Ｈｕｎｇ－Ｍｉｎらによる特許文献４は、ネットワークで鍵を配布するための方法及びシステムを開示する。この方法及びシステムでは、ネットワークのノードが鍵管理を開始する。指定されたノードのうちの１つの鍵プールは隣接するノードによって利用されるため、ネットワーク内で伝搬する。
【００１２】
現状技術は以下の問題を抱えている。現状技術の解決法は、センサノード間のピアツーピア通信の存在を考慮に入れているが、これは現実に使用する用途のほとんどでは可能ではない場合もある。さらに、センサノードの数が増加すると、現状技術が提示するプライバシー保全アルゴリズムの計算が増加する。
【００１３】
実用的な現実のシナリオのほとんどにおいて、センサノードはピアツーピア通信モードを用いてお互いに直接通信することはできない。このような事例では、現状技術で開示している方法は有用ではない。
【００１４】
たとえば、テレビ視聴率（ＴＲＰ）計算のプライバシーを保全した計算を考慮すると、センサノード間のピアツーピア通信の存在及びプライバシー保全アルゴリズムの計算の複雑さが増加することに関する現状技術の制限によって、ＴＲＰを計算する際に現状技術が有用ではなくなる。
【００１５】
ＴＲＰはチャンネルまたはプログラムの人気を示す基準であり、このデータは、ビジネ

ス上の効果が大きく、広告主にとっては非常に有用である。ＴＲＰは一般に、視聴者に関して集約したデータを準備して、様々な場所及び様々な時間における様々なチャンネルの統計を見つけることによって聴衆を頻繁に監視して、計算される。ＴＲＰ計算の概念として、個々の視聴者の統計は必要なく、特定のチャンネルの特定の場所で集約した視聴者の値で十分である。最も粗い形態で個々の視聴者が記録され、商業的用途のために利用される範囲がある。しかし、視聴者は、自分が見るチャンネルのパターンに関する情報を共有することを望まないこともある。そこで、サービスプロバイダ側での個々の視聴者データの集約には、プライバシーを保護することが必要となる。つまり、サービスプロバイダは視聴者のデータの個々の内容を具体的には知らないまま、視聴者のデータを集約する。

【００１６】

したがって、ＴＲＰ計算及び他の多くのアプリケーションなどのリアルタイムアプリケーションは、従来技術に記載する方法を用いて実行可能でないこともある。また、現状技術でＨｅ．Ｗらが提示する計算の複雑さは、ネットワーク内のセンサノード及びクラスタを追加することによって、急激に増加する。さらに、現状技術のいずれもが、センサノード間のピアツーピア通信モードがない無線センサネットワークでのデータ集約の間、データのプライバシーを保全するための方法を開示していない。さらに、現状技術が開示する方法は拡張性に欠け、高額な計算間接費用がかかる。

【００１７】

したがって、前述の従来技術に照らして、センサノード間のピアツーピア通信が存在しないネットワークにおいて、複雑ではなく、拡張性が高く、プライバシーを保全したデータ集約を計算する、新規な方法を提示するシステム及び方法の必要があることは明らかである。前述の従来技術に照らして、センサノード間のピアツーピア通信が存在しないことは、様々な現実の適用において、非常に現実的なシナリオである。

【先行技術文献】

【特許文献】

【００１８】

【特許文献１】米国特許出願第２００８０２４７５３９号

【特許文献２】米国特許出願第２００９０１４１８９８号

【特許文献３】米国特許第７７０２９０５号

【特許文献４】米国特許出願第２００８００４４０２８号

【非特許文献】

【００１９】

【非特許文献１】Ｈｅ．Ｗ．ｅｔ　ａｌ．、「ＰＤＡ：Ｐｒｉｖａｃｙ－ｐｒｅｓｅｒｖｉｎｇ　Ｄａｔａ　Ａｇｇｒｅｇａｔｉｏｎ　ｉｎ　Ｗｉｒｅｌｅｓｓ　Ｓｅｎｓｏｒ　Ｎｅｔｗｏｒｋｓ」、ＩＥＥＥ　ＩＮＦＯＣＯＭ、ｐｐ．２０４５－２０５３、ＩＥＥＥ　Ｐｒｅｓｓ、Ｎｅｗ　Ｙｏｒｋ（２００７）

【非特許文献２】Ｏｌｉｖｅｉｒａ、Ｓ．Ｒ．Ｍ　ｅｔ　ａｌ．、「Ａｃｈｉｅｖｉｎｇ　Ｐｒｉｖａｃｙ　Ｐｒｅｓｅｒｖａｔｉｏｎ　ｗｈｅｎ　Ｓｈａｒｉｎｇ　Ｄａｔａ　ｆｏｒ　Ｃｌｕｓｔｅｒｉｎｇ」、ＳＤＭ　２００４、ＬＮＣＳ、第４巻

【発明の概要】

【課題を解決するための手段】

【００２０】

本方法、システム、及びハードウェアイネーブルメントについて記載する前に、まず本発明は、記載する特定のシステム及び方法論に限定されない。本開示に明示的に例示されない、本発明の複数の可能性のある実施形態がありえるためである。また、本明細書で用いる用語は、特定のバージョンまたは実施形態を記載することのみを目的とするものであり、本発明の範囲を限定することを目的とするものではない。

【００２１】

本発明は、無線非階層センサネットワークにおける効率的で安全なデータ集約方式のための方法及びシステムを提供する。ネットワークは、クエリサーバに報告する複数のセン

サノードと、データのプライバシーを保全しながらセンサノードから送信されるデータを集約するサーバとを備える。本発明によって、サーバがセンサノードのデータの内容を取得することが回避される。本発明は、センサノード間のピアツーピア通信を必要とせず、多数のセンサノードが存在する場合であっても、平均して短い計算時間を有する。

【００２２】

本発明によって、センサノード間のピアツーピア通信がない場合の、センサノード間の効率的で自己適応型クラスタ形成が可能となり、無線センサネットワークでデータを集約中に、計算が複雑ではなく、拡張性が高いデータ保全アルゴリズムを提供する。

【００２３】

本発明は、センサノード間と、センサノードとサーバノード間との安全な通信をそれぞれ確立するためにセンサノード間と、センサノードとサーバノード間のロバストな対の鍵管理方式を提供する。

【００２４】

提示する本発明は、ＴＲＰ測定、スマートエネルギメータ読み込み通信などの実用的な事例において可能性のある用途を有する。

【図面の簡単な説明】

【００２５】

【図１】本発明の代表的な実施形態による、無線センサネットワークでの安全なデータ集約のための、様々なシステム要素を含有するシングルホップ無線センサネットワーク構造１００を概略的に示す説明図

【図２ａ】本発明の代表的な実施形態による、無線センサネットワークでの自己適応型クラスタ形成する次のステップを示すブロック図

【図２ｂ】本発明の代表的な実施形態による、無線センサネットワークでの自己適応型クラスタ形成する次のステップを示すブロック図

【図２ｃ】本発明の代表的な実施形態による、無線センサネットワークでの自己適応型クラスタ形成する次のステップを示すブロック図

【図３】本発明の代表的な実施形態による、本発明で提示するプライバシー保全アルゴリズムの計算に必要な計算時間と、現状技術の解決法に必要な計算時間との比較を示すグラフ

【図４ａ】本発明の代表的な実施形態による、無線センサネットワークでのサーバノードからシンク／センサノードへの鍵の確立と、安全な通信の次のステップを示すブロック図

【図４ｂ】本発明の代表的な実施形態による、無線センサネットワークでのサーバノードからシンク／センサノードへの鍵の確立と、安全な通信の次のステップを示すブロック図

【図４ｃ】本発明の代表的な実施形態による、無線センサネットワークでのサーバノードからシンク／センサノードへの鍵の確立と、安全な通信の次のステップを示すブロック図

【図５ａ】本発明の代表的な実施形態による、本発明で提示する私有データ開示の可能性と現状技術解決法による開示の可能性との比較を示すグラフ

【図５ｂ】本発明の代表的な実施形態による、本発明で提示する私有データ開示の可能性と現状技術解決法による開示の可能性との比較を示す説明図

【図５ｃ】共有鍵の数と１つの共通共有鍵の可能性との案計を示すグラフ

【図６】本発明の代表的な実施形態により、効率的で自己適応型なクラスタ形成を、無線センサネットワークでデータ集約中に形成するために実行するステップを説明するフローチャート６００

【図７】本発明の代表的な実施形態により、センサノードとサーバノードとの間の安全な通信を、無線センサネットワークでデータ集約中に確立するための事前配布段階を説明するフローチャート７００

【図８】本発明の代表的な実施形態により、ネットワークの複数のシンク／センサノードのうちの少なくとも１つと、サーバ／アグリゲータノードとの間の安全な通信を確立するステップを説明するフローチャート８００

【図９】本発明の代表的な実施形態により、ネットワークの２つのシンク／センサノード

間の安全な通信を確立するためのステップを説明するフローチャート９００
【発明を実施するための形態】
【００２６】
前述の概要、ならびに後述の好ましい実施形態の詳細な説明は、添付図と合わせて読むとよりよく理解される。本発明を例示するために、図には本発明の例示構成を示す。ただし、本発明は図中で開示する特定の方法及び構造に限定されない。
本発明の一部の実施形態を、その特徴を例示しながらここで説明する。
【００２７】
「備える」、「有する」、「含有する」、及び「含む」という用語、ならびにその変化形は、これらの用語のいずれか１つに続く１または複数の項目がその１または複数の項目の排他的な一覧であることを意味するものではなく、または一覧に挙げられた１または複数の項目にのみ限定されることを意味するものではないという点で、意味的には同等であり、制約がないことを意図する。
【００２８】
また、本明細書及び添付の請求項で用いるように、単数形の「１つの」及び「その」という用語は、別段明示しない限り、複数形も含むことに注意すべきである。本明細書に記載するシステム、方法、機器、及び装置と類似する、または同等である任意のシステム、方法、機器、及び装置は、本発明の実施形態の実行または試験において用いることができるものの、好ましいシステム及び部品をここで記載する。開示する実施形態は単に本発明の代表例であり、様々な形態で実施してもよい。本発明の範囲は一覧に挙げた実施形態には限定されず、添付の請求項によってのみ限定される。
【００２９】
本発明は、ネットワークのセンサノード間にはピアツーピア通信が存在しない無線センサネットワークにおいて時間効率の良い自己適応型クラスタ形成を可能にし、複雑ではなく、拡張性の高いプライバシーを保全したデータ集約を提供する。
【００３０】
図１は、簡易プライバシー保全データ集約（ＳＰＰＤＡ）モデルと称するシングルホップ無線センサネットワーク（ＷＳＮ）１００を参照する。シングルホップ無線センサネットワーク（ＷＳＮ）１００は、本発明の代表的な実施形態による、無線センサネットワークでのデータ集約のタスクを集合的に実現する様々なハードウェア要素からなる。
【００３１】
本発明の実施形態では、図１に示すように、システム１００は、３つの種類のノードを無線センサネットワークに含む。
３つの種類のノードは、基地局（ＢＳ）１０１、サーバ／アグリゲータノード１０２及びシンク／センサノード１０３－１、１０３－２、１０３－３……１０３－Ｎを含む。サーバ／アグリゲータノード１０２はデータ集約機能を実行し、集約したデータをさらに処理し、次に、結果をＢＳ１０１に送信する。サーバノード１０２は、サーバノード１０２と無線リンクｄ（１）、ｄ（２）、ｄ（３）…．ｄ（Ｎ）を通じて接続するＮ個のシンク／センサノード１０３－１…１０３－Ｎと接続を有する。図１に示すシングルホップ無線センサネットワーク（ＷＳＮ）１００において、シンク／センサノード間にピアツーピア通信は存在しないと考えられる。単一のＷＳＮ１００は大規模なマルチホップＷＳＮのサブセットと考えられるが、簡略化するために、シングルホップＷＳＮを説明のために想定する。
【００３２】
シンク／センサノードは、それ自体で、またはサーバ／アグリゲータノード１０２からの指示によってデータを収集する。ネットワークのシンク／センサノードは、ピアツーピア接続を持たないものと考えられる。したがって、複数のセンサノードのうちの１つが別のシンク／センサノードと通信を確立しようとする場合は、サーバ／アグリゲータノード１０２を通じて行わなければならない。その結果として、現状技術が直面していた拡張不能である問題が排除される。

【００３３】
ネットワークの別のシンク／センサノードと通信するために、シンク／センサノードは、サーバ／アグリゲータノード１０２に要求する。サーバノード１０２は、フォワーダ機能を実行する。
【００３４】
プライバシー保全ポリシーを実装するために、１つのシンク／センサノードは、ネットワークの別のセンサノードと通信する必要がある。これは、対になる鍵を確立する技術によって安全に行われる。ただし、ＴＲＰ計算などの実用的なシナリオのほとんどでは、この対になる鍵を確立すること、及びシンク／センサノード間で直接通信することは不可能である。
【００３５】
提示されたＳＰＰＤＡモデル１００は、効率的なプライバシー保全アルゴリズムを実装する。このアルゴリズムは、センサノード間のピアツーピア通信の制限を効率的な自己適応型クラスタ形成によって克服し、本明細書で詳細に後述するロバストな鍵管理方式によって安全性の問題を確実にする。
【００３６】
図１に示すＳＰＰＤＡモデルでは、サーバノード１０２と、シンク／センサノード１０３－１…１０３－Ｎそれぞれとの間の通信はデータ損失がなく正確であると考えられる。さらに、シンク／センサノードは常に、サーバ／アグリゲータノード１０２の通信範囲内であると考えられる。サーバノード１０２はシンク／センサノードのうち１つと隣接するシンク／センサノードに、その特定のシンク／センサノードとサーバノード１０２との通信に障害がある場合は通知する。
【００３７】
図２（ａ）、（ｂ）及び（ｃ）はブロック図を示し、効率的な自己適応型クラスタをシングルホップ無線センサネットワークに形成することを示す。
システムの拡張性を提供し、ノード間の通信を確保し、プライバシー開示の可能性を最小にするために、効率的なクラスタ形成が必要である。このクラスタ形成によって、シンクツーシンク通信の安全性が提供され、最終的には、プライバシー保全アルゴリズムを直接的なシンクツーシンク通信を用いずに無事に実行することにつながる。これらのシンクノードはデータを収集してサーバに送信する。クラスタ形成アルゴリズムは以下の通りである。
【００３８】
図２（ａ）は本発明の実施形態におけるクラスタ形成の第１のステップを示す。
サーバ／アグリゲータノード２０１は「ハロー」メッセージをネットワークの複数のシンク／センサノード２０２に配布する。次に、サーバノード２０１はシンク／センサノードからの肯定応答を待つ。サーバ／アグリゲータノード２０１から配布された「ハロー」メッセージに対する応答を、複数のシンク／センサノードの一部から受信すると、サーバは、ネットワーク内のアクティブなノードが分かるようになる。
【００３９】
図２（ｂ）は、本発明の実施形態におけるクラスタ形成の第２のステップを示す。
図２（ｂ）に示すサーバ／アグリゲータノード３０１は、第１のステップで認識されたアクティブなノードを分割して、クラスタのグループを形成する。各クラスタは、収集したデータをサーバ／アグリゲータノード３０１に報告する４つのアクティブシンク／センサノードからなる。したがって、ネットワークにはＮ／４個のクラスタが形成され、Ｎはネットワークのアクティブなシンク／センサノードの数と等しい。ただし、Ｎ／４が整数ではない場合は、ネットワーク内に５つのアクティブなノードから形成される少数のクラスタがある場合もある。５つのアクティブなノードを備えるクラスタの数は３以下であることが観測されている。
【００４０】
図２（ｂ）に示すように、「クラスタ１」３０２は４つのシンク／センサノードで形成

される。同様に、ネットワークの別のシンク／センサノードはクラスタに分割され、各クラスタは４つのアクティブなシンク／センサノードを備える。クラスタ形成情報は、別のネットワークのシンク／センサノード間でサーバ／アグリゲータノード３０１によって共有される。これらの別のシンク／センサノードは、シンク／センサノードが属するクラスタの近隣と称される。たとえば、図２（ｂ）では、シンク／センサノード３０３－１、３０３－２、３０３－３及び３０３－４はクラスタ１　３０２に属し、この情報は、サーバ／アグリゲータノード３０１によってこれらのノードそれぞれで共有される。

【００４１】

サーバ／アグリゲータノード３０１は、クラスタ内のシンク／センサノード対を選択し、シンク／センサノード対の形成に関する情報をクラスタ内の別のシンク／センサノードに伝える。

【００４２】

たとえば、本発明の実施形態において、図２（ｃ）に示すクラスタ形成図を考慮する。サーバ／アグリゲータノード（図２（ｃ）には不図示）は、シンク／センサノード１　４０１及びシンク／センサノード２　４０２を選択して、「対１１」をクラスタ１　４００から形成する。同様に、サーバ／アグリゲータノード（図２（ｃ）には不図示）は、シンク／センサノード３　４０３及びシンク／センサノード４　４０４を選択して、「対２１」をクラスタ１　４００から形成する。このようにして、サーバ／アグリゲータノードは２つのアクティブなシンク／センサノードを各クラスタから選択して、対を形成する。この原則によって形成された対はフレンド対（ｆｒｉｅｎｄ　ｐａｉｒ）と称される。

【００４３】

実施形態では、サーバ／アグリゲータノードは、定期的に「ハロー」メッセージを配布することによって、シンク／センサノードの状態を頻繁に監視する。任意のシンク／センサノードが、受信したメッセージに応答することを繰り返し失敗する場合には、そのノードはサーバ／アグリゲータノードによって、パッシブまたはデッドノードと考えられる。この状況は、サーバ／アグリゲータノードによるフレンド対形成の再グループ化につながり、その結果として、３つのシンク／センサノードを１つの対に含む場合もある。サーバノードは次に、フレンド対形成のこの調整または再グループ化を対応するシンク／センサノードに通知する。サーバノードの目的は形成後にクラスタを妨害しないことである。このシナリオでは、別のノードがネットワークに入ると、サーバノードは、クラスタのうちの１つが４未満のノードを有する場合は、ノードをそのクラスタに収容しようとする。そうでなければ、そのノードをクラスタのうちの１つに一時的に収容する。あるクラスタに一時的に収容されるこのようなシンクノードのうちの４つが利用可能であるとき、この４つは新しいクラスタを形成する。

【００４４】

無線センサネットワークでのこの自己適応型で効率的なクラスタ形成機構によって、ネットワークにおける計算が複雑でなくなる。Ｈｅ．Ｗらが提示した従来技術の計算の複雑さは、シンク／センサノード及びクラスタをネットワークに追加すると急激に増加する。本発明のクラスタ形成機構では、計算の複雑さは固定され、ネットワークのシンク／センサノードの数には影響されない。本発明で提示するＳＰＰＤＡ方式における様々な数のノードに必要な計算時間を、行った実験に基づいて、Ｈｅ．ＷらのＣＰＤＡ方式と比較した。その結果を表１に示す。

【００４５】

【表１】

ＳＰＰＤＡ	ＣＰＤＡ	センサノードの数
４０	２２０	３
５０	２５０	４
５１	３１０	５

ＳＰＰＤＡ及びＣＰＤＡの様々な数のノードでの計算時間
（単位：１０００分の１秒）

【００４６】
表１から、シンク／センサノードの数が増加するとき、ＳＰＰＤＡの計算時間はほとんど一定である一方、ＣＰＤＡの計算時間はより急速に増加することが観測される。
【００４７】
これは図３でもさらに示され、ＳＰＰＤＡにおいて、計算時間はＣＰＤＡより大幅に短いことも分かる。これらの２つの方式の間の計算時間の相違は、考慮するノードの数が増加すると、より明らかになる。これは、ＳＰＰＤＡでは、ほとんどの場合に（３つのシンクノードがクラスタを形成してもよい、一定のシンクノードの故障を考慮に入れない）、プライバシーを保全した計算に関与する固定された２つの数のシンクノードがあるため、計算時間が固定されるためである。これは、全体的なシステムが本質的にリアルタイムであるとき、実際に必要な要件である。ＣＰＤＡアルゴリズムでは、ノードの数が追加されると、計算時間はほとんど線形に増加する一方、ＳＰＰＤＡでは、非常に低い計算負荷しか生じず、クライアント／シンクノードの数が追加されてもあまり影響は受けない。ＣＰＤＡでは、ノードの数が増加すると計算時間は増加するが、一方、本発明が提示するＳＰＰＤＡでは、シンク／センサノードの数は５つに限定される。また、ＣＰＤＡでは、単一のクラスタに多数のシンクノードを有することは非現実的である。
【００４８】
シンクノードから対応するアグリゲータまたはサーバに送信されるメッセージのプライバシー及び統合性を確保するための支持を提供するために、ロバストな鍵交換及び管理方式が必要である。本発明の実施形態では、ロバストな対の鍵管理方式を設計し、鍵をセンサノード（シンクノード及びサーバを含む）に選択的に配布し、そこから削除することによって、ならびに大量の計算または帯域幅を使用せずにノードに再度鍵をかけることによって、非階層のシングルホップセンサネットワークの操作性及び安全性要件を満たす。提示する鍵管理方式の目的は以下の通りである。
・ネットワーク内でデータを安全に交換しなくてはならないすべてのセンサノード間の鍵を確立すること。
・ネットワーク内のノードの追加または削除を支持すること。
・画定されていない配備環境で鍵管理方式の動作を可能にすること。
・認証されていないノードがネットワーク内の任意の別のノードと通信できないようにすること。
【００４９】
これらの目的を達成するために、第１のステップではシンク／センサノードのクラスタを形成する。Ｎ個のシンク／センサノードがあり、各クラスタはｎ個のシンク／センサノードからなると考えられる。すると、Ｎ／ｎ個のクラスタがあることになる。鍵管理方式は鍵の事前配布段階によって開始する。事前配布段階では、Ｋ個の鍵の大量の鍵のプールと、それに対応する識別情報を生成する。これらのＫ個の鍵は２つのバンクに分割される。第１のバンクはｋ個の鍵からなり、アグリゲータノードを介してシンク／センサノードと別のシンク／センサノードとの通信に用いられる。第２のバンクは（Ｋ－ｋ）個の鍵からなり、シンク／センサノードとアグリゲータ／サーバノードとの通信に用いられる。
【００５０】
したがって、２つの部品からなる鍵管理方式を以下で説明する。
【００５１】
第一部：シンク／センサノードからアグリゲータ／サーバノードまでの鍵を確立する。
本発明の実施形態では、各シンク／センサノードはＫ－ｋ個の鍵をサーバと共有して有する。すべてのシンク／センサノードが同じ鍵を所有するため、シンク／センサノードがサーバ／アグリゲータノードと共有鍵を用いて通信することは極めて危険である。任意の悪意のあるシンク／センサノードは、シンク／センサノードとサーバとの通信を解読する

ことができ、非常に簡単に攻撃を開始することができる。これを避けるために、事前配布段階において、シンク／センサーサーバの鍵バンクはシンク／センサーサーバ対ごとにランダムに順序が変えられ、並べ変えられる。鍵バンクのこの順序は各シンク／センサノードのサーバノードに記憶される。これを図４（ａ）に示す。

【００５２】

新しいシンク／センサノードがネットワークに追加されると、前述した鍵バンクランダム化と同一の手順が行われ、新しいシンク／センサノードに対する鍵の順序がオフラインで記憶される。ここで、シンク／センサノードは、その共有鍵のうちの１つを通じて、サーバノードと通信する。この動作を達成するために、シンク／センサノードはまず、１から（Ｋ－ｋ）までの間でランダムな数を生成する。このランダムな数（Ｒｃ）はプレーンテキストでサーバに送信される。サーバは、シンク／センサノードが次のメッセージを鍵バンクのＲｃ番目の鍵で暗号化することを理解する。サーバノードはＡＣＫ（肯定応答）を送信して応答する。これを図４（ｂ）に示す。

【００５３】

ＡＣＫ（肯定応答）を受信後、シンク／センサノードはデータを特定の鍵で暗号化して、サーバノードに送信する。シンク／センサノードがサーバノードと通信することを望むときは毎回、同じステップを取る。これを図４（ｃ）に示す。各セッションで、ランダムな数を生成するプロセスによって、推測による攻撃を防ぐ。ランダムな数（Ｒｃ）がシンク／センサノードにプレーンテキストで送信されることも観測することができる。しかし、これによって、任意の脆弱性の問題は発生しない。悪意のあるノードがランダムな数を入手しても、鍵バンク順序を事前にランダム化することによって、危害を受けることはないからである。異なるシンク／センサノードでは、Ｒｃ番目の鍵は異なる。事前配布段階で、マッピングはサーバノードにオフラインで記憶される。

【００５４】

第二部：シンク／センサノードからシンク／センサノードまでの鍵を確立する。

本発明の実施形態では、シンク／センサノードから別のシンク／センサノードへの直接通信は存在せず、この通信はサーバ／アグリゲータノードを通じて行われると考えられる。さらに、サーバノードは、シンク／センサノード間の通信を解読すべきではないことにも留意されたい。そうでないとすると、プライバシー保全アルゴリズムはサーバノードにとって、解読するには些細なものとなる。これを実現するために、ｋ個の鍵をシンクノード配備時に事前に記憶させるが、サーバノードには記憶させない。サーバは、サーバノードからシンク／センサノードへの通信には（Ｋ－ｋ）個の鍵が必要であることのみを認識している。

【００５５】

ネットワークの別のシンク／センサノードは、ネットワークでシンク／センサノードの１つから別のシンク／センサノードに送信されるメッセージを解読すべきではないということも要件である。たとえば、シンク／センサノード１がシンク／センサノード２との通信を望み、ｋ個の鍵がネットワークのすべてのシンク／センサノードで同じである場合は、別のシンク／センサノードがプレーンテキストを復号化することが容易になる。つまり、シンク／センサノード３は、シンクノード１とシンク／センサノード２が通信していることを復号化することができる。

【００５６】

この状況を避けるために、シンク／センサノード１及びシンク／センサノード２は個別にシンク／センサノードからシンク／センサノードへの通信専用のｋ個の鍵の鍵バンクの順序を変え、ランダムに並べ変える。鍵バンクのランダムな順序変えに続き、シンク／センサノード１及び２は、サーバノードと対になる鍵を用いて、順序を変える機能を、サーバノードを通じてお互いに送る。

【００５７】

順序を変える機能を無事に配送すると、シンク／センサノードのうちの１つ（たとえばシンク／センサノード１）は、１からｋまでの間の別のランダムな数を別のシンク／セン

サノード（たとえばシンク／センサノード２）に送信する。この別のランダムな数は、順序を変えた鍵バンクの特定の鍵を示す。シンク／センサノード間のこの対になる鍵を用いて、データ集約が完了するまでその後の通信を行う。データ集約プロセスの次のラウンドでは、鍵を確立する同じ手順が取られる。

【００５８】

このロバストな対の鍵管理方式によって、個々のシンク／センサノード間の安全な通信、及びシンク／センサノードのうちの１つとサーバノード間との通信が、個々のシンク／センサノードのデータの私有内容を損失することなく可能となる。これによって、通信ノード間にピアツーピア通信がないネットワークでデータを集約する際に、プライバシーを保全することを支援する。認証されていない、または悪意のあるノードに対して、個々のシンク／センサノードの私有データが開示される可能性はない。

【００５９】

現状技術においてＨｅ．Ｗらが提示したＣＰＤＡ方式では、私有データが開示されるかもしれない一定の可能性が存在する。これは、シンクノードがメッセージをクラスタ内で交換するときにのみ発生し得る。これは次式から推測できる。

【００６０】

【数１】

$$P(b) = \sum_{m=pc}^{Dmax} P(k=m)\left(1-\left(1-b^{m-1}\right)^{m}\right)$$

【００６１】

式中、Ｄｍａｘ＝最大クラスタサイズ、

ｐｃ＝最小クラスタサイズ（＝２、２つのシンクノード）、

ｋ＝クラスタサイズ、

ｂ＝リンクレベルのプライバシーが解読される可能性

Ｐ（ｋ＝ｍ）＝クラスタサイズがｍである可能性

である。

【００６２】

ここで、本発明が提示するＳＰＰＤＡ方式では、

ｐｃ＝Ｄｍａｘ＝ｋ＝２、したがってＰ（ｋ＝ｍ）＝１である。

【００６３】

したがって、ＣＰＤＡで解読されるプライバシーの確率はＳＰＰＤＡで解読されるプライバシーの確率よりもはるかに傾斜が急であることが分かる。図表を図５（ａ）に示す。

【００６４】

ＣＰＤＡでは、シンク／センサノードの対が同じ鍵の対を所有するという要件は高くなるはずである。鍵はランダムに大規模な鍵のプールから選択される。そうではない場合は、この方式は機能しない。しかし、この要件によって、別のノードが共通の鍵の対を有する場合は、別のノードは少なくとも通信の一部を取得することができる。

【００６５】

図５（ｂ）のシナリオを考慮することにする。図示するように、３つのノード、つまりノード１、ノード２及びノード３がある。ノード１とアグリゲータ／サーバノード間の鍵はＭ１であり、ノード２とアグリゲータ／サーバノード間の鍵はＭ２である。同様に、ノード３とアグリゲータ／サーバノード間の鍵はＭ３であり、ノード４とアグリゲータ間の鍵はＭ４である。

【００６６】

ＣＰＤＡのノード間で同じ鍵が共有されてもよい一定の可能性（非常にわずかであるとしても）もあることが観測される。たとえば、ノード１とアグリゲータ／サーバノード間とで共有する鍵は、ノード２とアグリゲータ／サーバノード間の鍵と同じである（つまり、Ｍ１＝Ｍ２）。これは、一定のユースケースにおいて厳格な安全性要件に違反する。実

際に、ＣＰＤＡ方式では、ノード間で鍵を共有する確率は、ネットワークのシンク／センサノードの数が増えるにつれて増加する。

【００６７】

ただし、ＳＰＰＤＡでは、鍵配布は完全に決定論的であり、ネットワーク内での安全性に関する脆弱性問題を回避する。ただし、これは、鍵プール内の鍵の数を増加させることにつながることもある。さらに、本発明で提示する鍵管理方式では、鍵配布プロセスは完全にランダム化され、ノードのフレンド対をクラスタに形成することはアグリゲータ／サーバノードによって制御される。

【００６８】

フレンド対を形成するノードの数は、サーバによって決定され、ほとんどの場合は理想的には２である。ただし、シンク／センサノードのうちの１つがパッシブまたはデッドとなる場合を除く。したがって、ノードの対が共通鍵を発見することが決定論的ではないというこの種の状況を排除することによって、ＳＰＰＤＡは、様々な攻撃に対してはるかに安全でロバストになる。

【００６９】

図６はフローチャート６００であり、本発明の実施形態により、効率的で自己適応型なクラスタ形成を無線センサネットワークでデータ集約中に形成するために実行するステップを説明する。

【００７０】

ステップ６０１では、連続してサーバ／アグリゲータノードは、「ハロー」メッセージをネットワークで定期的に配布する。

【００７１】

ステップ６０２では、サーバノードは、ステップ６０１で配布したメッセージに対する応答を待つ。

【００７２】

ステップ６０３では、サーバノードは、ネットワークの任意のノードから任意の応答があるかどうかを監視または追跡する。

【００７３】

ステップ６０４では、ネットワークのアクティブノードは、サーバノードのメッセージに応答したものとして認識され、クラスタにグループ化される。各クラスタは４つまたは５つのアクティブなノードを備える。

【００７４】

ステップ６０５では、サーバノードは、２つのノードを各クラスタから選択し、それらをグループ化して、フレンド対を形成し、ネットワークの各クラスタに２つのフレンド対を形成する。

【００７５】

図７はフローチャート７００であり、本発明の実施形態により、センサノードとサーバノードとの間の安全な通信を無線センサネットワークでデータ集約中に確立するための事前配布段階を説明する。

【００７６】

ステップ７０１では、識別情報を備えて生成された多数の鍵（Ｋ）のプールを維持する。

【００７７】

ステップ７０２では、Ｋ個の鍵からなるプールを、ｋ個及びＫ－ｋ個の鍵をそれぞれ有する２つのバンクに分割する。

【００７８】

ステップ７０３では、Ｋ個の鍵のプールをランダムにネットワークの複数のシンク／センサノード間で配分する。

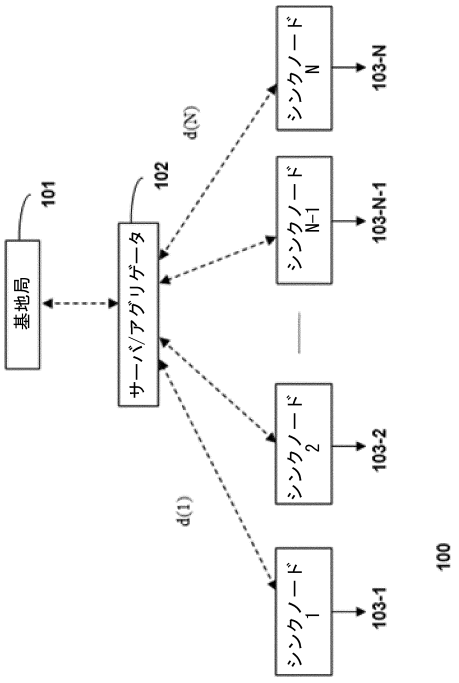
【００７９】

ステップ７０４では、ｋ個の鍵を備える鍵バンクは、ネットワークのシンク／センサノ

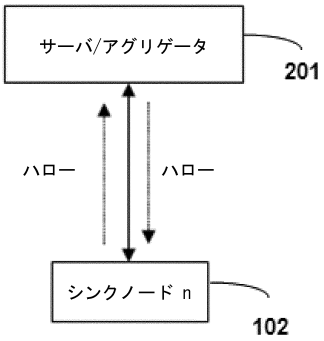
ードのそれぞれで共有され、記憶される。
【００８０】
ステップ７０５では、Ｋ－ｋ個の鍵を備える鍵バンクは、サーバ／アグリゲータノードで共有され、記憶される。
【００８１】
図８はフローチャート８００であり、本発明の実施形態により、ネットワークの複数のシンク／センサノードのうちの少なくとも１つとサーバ／アグリゲータノードとの間の安全な通信を確立するステップを説明する。
【００８２】
ステップ８０１では、Ｋ－ｋ個の鍵を備える鍵バンクを、ランダムに順序を変え、並べ変え、サーバ／アグリゲータノードに記憶する。
【００８３】
ステップ８０２では、シンク／センサノード自体がサーバ／アグリゲータノードで集約するために収集したデータを送信することを望む場合、シンク／センサノードは１から（Ｋ－ｋ）までの間のランダムな数（Ｒｃ）を生成する。
【００８４】
ステップ８０３では、シンク／センサノードは生成したランダムな数（Ｒｃ）をサーバ／アグリゲータノードにプレーンテキストの形式で送信する。
【００８５】
ステップ８０４では、サーバノードはランダムな数の受信を確認し、通信を望むシンク／センサノードが、生成したランダムな数に対応する鍵で共有すべきデータを暗号化することを確認し、したがって、通信を開始したシンク／センサノードにＡＣＫ信号を送信する。
【００８６】
ステップ８０５では、シンク／センサノードは、生成したランダムな数に対応する（Ｋ－ｋ）個の鍵のうち１つを選択する。
【００８７】
ステップ８０６では、シンク／センサノードは、サーバに送信すべきデータを選択した鍵で暗号化し、安全な通信及びプライバシー保全を可能にする。
【００８８】
図９はフローチャート９００であり、本発明の実施形態により、ネットワークの２つのシンク／センサノード間の通信をサーバ／アグリゲータノードを介して安全に確立するためのステップを説明する。
【００８９】
ステップ９０１では、シンク／センサノード１及び２はお互いに通信に関与し、それらの場所に記憶されるｋ個の鍵を備える鍵バンクの順序を変え、並べ変える。
【００９０】
ステップ９０２では、シンク／センサノード１及び２は、サーバノードを介して、サーバノードと対になる自分の鍵を用いて、順序を変える機能をお互いに対して送る。
【００９１】
ステップ９０３では、シンク／センサノード１はランダムな数をシンク／センサノード２に送信し、安全な通信を確立するための鍵の数を指示する。
【００９２】
ステップ９０４では、送信されたランダムな数に対応するｋ個の鍵のうちの１つを選択する。
【００９３】
ステップ９０５では、シンク／センサノード１は、シンク／センサノード２に送信すべきデータを、そのデータを選択した鍵で暗号化することによって送信する。
【００９４】
このように、自己適応型クラスタ形成及び対になる鍵管理方式によって、ピアツーピア

通信モードがネットワークの複数のシンク／センサノード間で存在しないネットワークにおいて、効率的なプライバシー保全アルゴリズムが可能となる。本方法では、２つのノードが、ネットワークの異なる領域で収集されたデータを共有するためにお互いに通信するとき、プライバシー保全アルゴリズムを実装するために複雑な計算は必要なく、第三者と鍵を共有することが回避される。

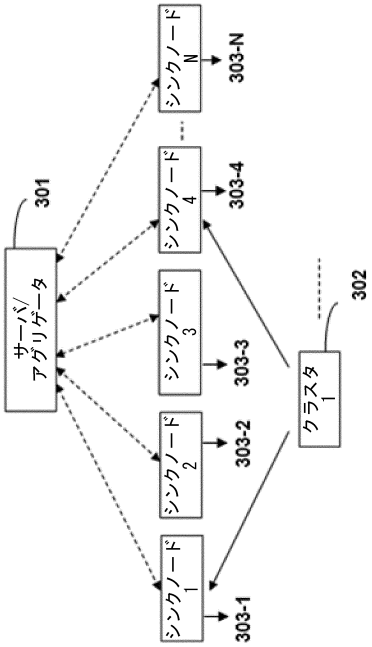
【図１】



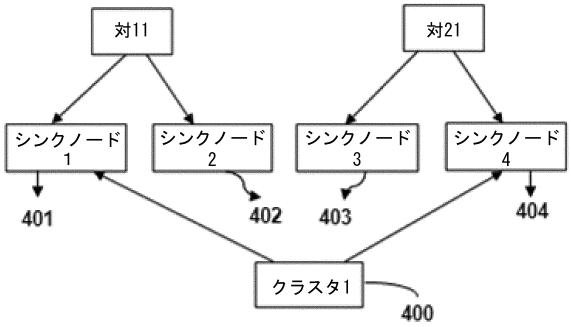
【図２ａ】



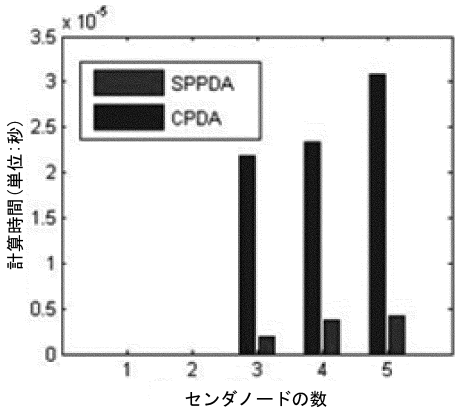
【図２ｂ】



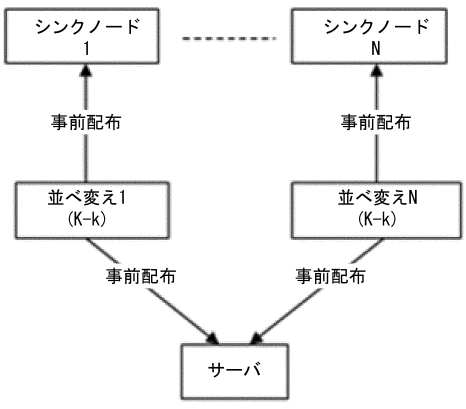
【図２ｃ】



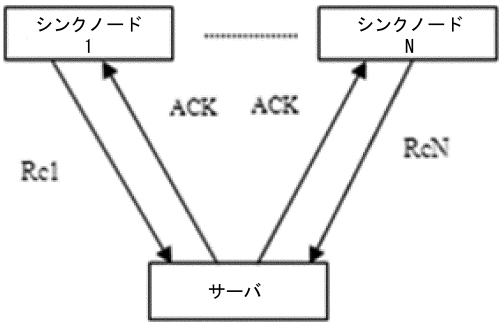
【図３】



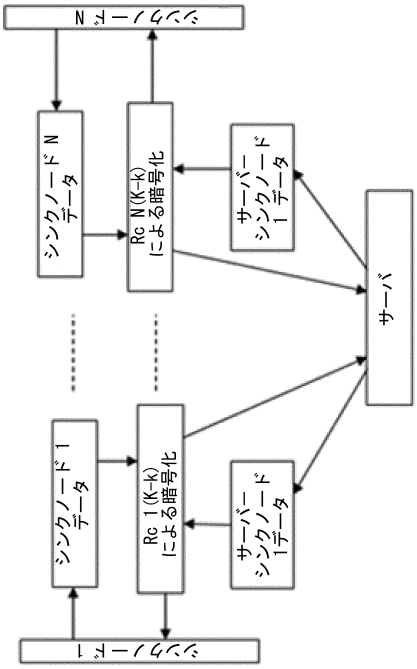
【図４ａ】



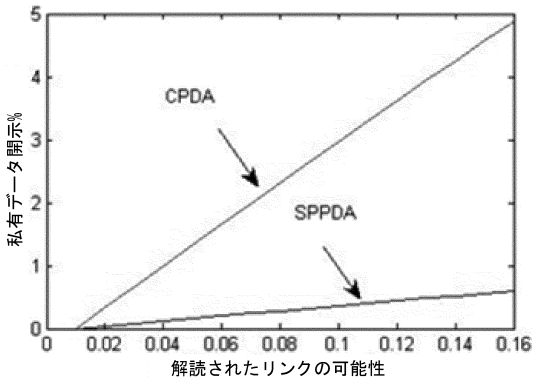
【図４ｂ】



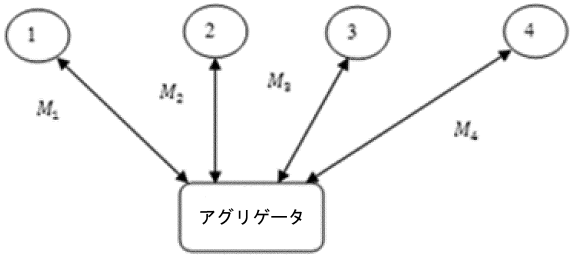
【図４ｃ】



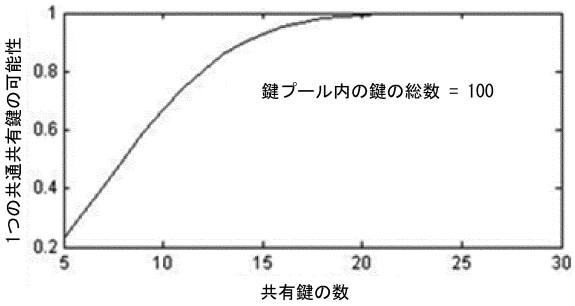
【図５ａ】



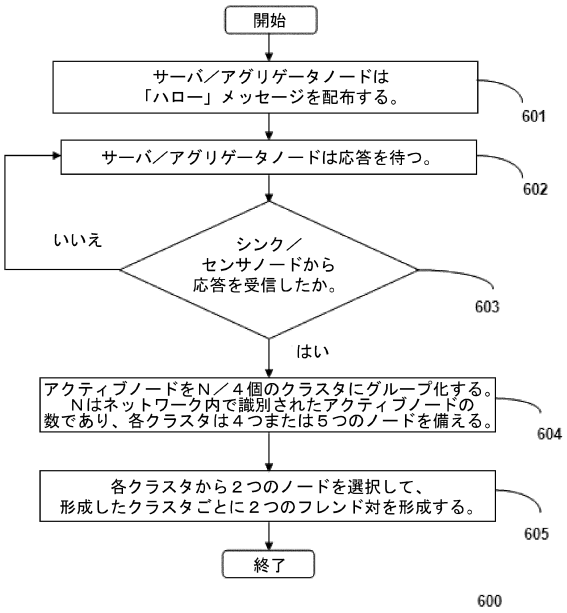
【図５ｂ】



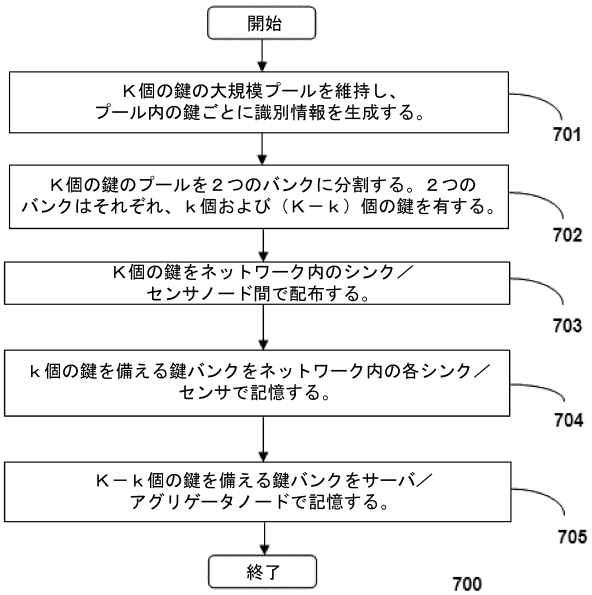
【図５ｃ】


1つの共通共有鍵の可能性
1
0.8
0.6
0.4
0.2
5
10
15
20
25
30
鍵プール内の鍵の総数 = 100
共有鍵の数

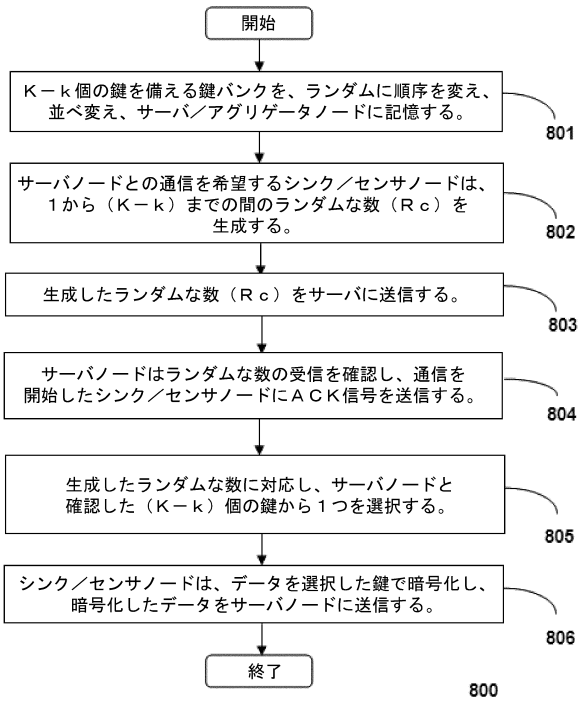
【図６】


開始
サーバ／アグリゲータノードは
「ハロー」メッセージを配布する。
601
サーバ／アグリゲータノードは応答を待つ。
602
いいえ
シンク／
センサノードから
応答を受信したか。
603
はい
アクティブノードをＮ／４個のクラスタにグループ化する。
Ｎはネットワーク内で識別されたアクティブノードの
数であり、各クラスタは４つまたは５つのノードを備える。
604
各クラスタから２つのノードを選択して、
形成したクラスタごとに２つのフレンド対を形成する。
605
終了
600

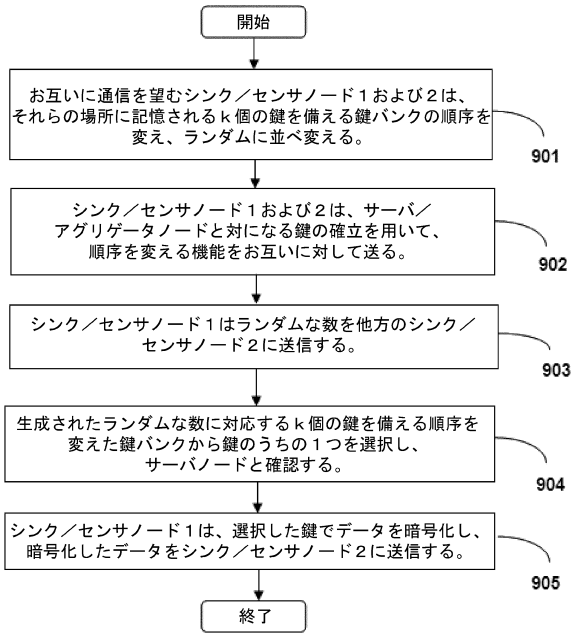
【図７】


開始
Ｋ個の鍵の大規模プールを維持し、
プール内の鍵ごとに識別情報を生成する。
701
Ｋ個の鍵のプールを２つのバンクに分割する。２つの
バンクはそれぞれ、ｋ個および（Ｋ－ｋ）個の鍵を有する。
702
Ｋ個の鍵をネットワーク内のシンク／
センサノード間で配布する。
703
ｋ個の鍵を備える鍵バンクをネットワーク内の各シンク／
センサで記憶する。
704
Ｋ－ｋ個の鍵を備える鍵バンクをサーバ／
アグリゲータノードで記憶する。
705
終了
700

【図８】


開始
Ｋ－ｋ個の鍵を備える鍵バンクを、ランダムに順序を変え、
並べ変え、サーバ／アグリゲータノードに記憶する。
801
サーバノードとの通信を希望するシンク／センサノードは、
１から（Ｋ－ｋ）までの間のランダムな数（Ｒｃ）を
生成する。
802
生成したランダムな数（Ｒｃ）をサーバに送信する。
803
サーバノードはランダムな数の受信を確認し、通信を
開始したシンク／センサノードにＡＣＫ信号を送信する。
804
生成したランダムな数に対応し、サーバノードと
確認した（Ｋ－ｋ）個の鍵から１つを選択する。
805
シンク／センサノードは、データを選択した鍵で暗号化し、
暗号化したデータをサーバノードに送信する。
806
終了
800

【図９】


開始
お互いに通信を望むシンク／センサノード１および２は、それらの場所に記憶されるｋ個の鍵を備える鍵バンクの順序を変え、ランダムに並べ変える。
901
シンク／センサノード１および２は、サーバ／アグリゲータノードと対になる鍵の確立を用いて、順序を変える機能をお互いに対して送る。
902
シンク／センサノード１はランダムな数を他方のシンク／センサノード２に送信する。
903
生成されたランダムな数に対応するｋ個の鍵を備える順序を変えた鍵バンクから鍵のうちの１つを選択し、サーバノードと確認する。
904
シンク／センサノード１は、選択した鍵でデータを暗号化し、暗号化したデータをシンク／センサノード２に送信する。
905
終了

フロントページの続き

(72)発明者　ウキル、アリジット
インド国　コルカタ　７００　０９１、ソルト　レイク、セクター－５、ビーアイピーエル、タタ　コンサルタンシー　サービシズ、イノヴェーション　ラブズ、タタ　コンサルタンシー　サービシズ
(72)発明者　セン、ジャイディップ
インド国　コルカタ　７００　０９１、ソルト　レイク、セクター－５、ビーアイピーエル、イノヴェーション　ラブズ、タタ　コンサルタンシー　サービシズ

審査官　打出　義尚

(56)参考文献　国際公開第２００２／０７６０１１（WO，Ａ１）
米国特許出願公開第２００８／０２４７５３９（ＵＳ，Ａ１）
米国特許出願公開第２００９／０２６８９１４（ＵＳ，Ａ１）
Siu-Ping Chan, Radha Poovendran, Ming-Ting Sun, A key management scheme in distributed sensor networks using attack probabilities, Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE (Volume:2), IEEE, ２００５年, pp. 1007-1011

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／１４