情報処理学会論文誌 Vol. 52 No. 3 1160–1172 (Mar. 2011)

複数の大規模グループに同時参加するセンサノード向けグループ鍵管理方式

野田 潤[†1,†2] 楫 勇一[†2] 中尾 敏康[†1]

センサネットワークの多くの応用は安全なグループ通信を要求する．1 つ以上の属性を共有するノードが同じグループに属すると考えるとき，ノードは一般に複数の属性を持つと考えられるため，1 台のノードは複数のグループに同時に属することになる．グループと安全な通信を行うためには，グループ内で共有させるグループ鍵の管理が重要となる．センサネットワークに適用可能なグループ鍵管理方式の研究がすでにいくつか行われている．しかし，安全にグループ鍵を管理するうえでの大きな問題として，1 台のノードが複数の大規模グループに所属する場合に，メモリ負荷と通信負荷が著しく増加することがあった．本論文では，複数ノードの内部情報が同時流出しない環境を仮定し，属性に紐つける管理情報を用いて，個々のグループ鍵の管理の仕組みを互いに連携させることで，従来に比べ，管理上の負荷を低減可能なグループ鍵管理方式を提案する．さらに適用例を与え，既存方式より，ノードのメモリ負荷の 64%〜88%を，通信負荷の 46%〜97%を削減できることを示す．

A Group Key Management Scheme for Sensor Nodes Belonging to Multiple Large-scale Groups

Jun Noda,[†1,†2] Yuichi Kaji[†2] and Toshiyasu Nakao[†1]

To realize secure communication between a server and groups of sensor nodes in a wireless sensor network, it is important to manage a group key that is shared among member nodes in a group. Several group key management schemes in sensor networks have been proposed. However, if a node belongs to multiple groups, both of the memory and communication costs increase according to the number of groups. In this paper, we propose a new scheme in which group keys of different groups help each other's key management in an environment of a number of nodes do not expose their important internal information at once. It is shown by an example scenario that our proposed scheme can eliminate 64%–88% of node's memory costs and 46%–97% of server's communication costs for managing multiple group keys compared to other known schemes.

1. はじめに

センサネットワークとは，センサ機能と通信機能を備える端末（ノード）と，ノードからの情報収集やセキュリティ確保を含むネットワークの管理を司る管理者（サーバ）から構成されるネットワークである．我々の生活空間や企業活動の現場に様々なセンサや端末が組み込まれ，それらがいつでもどこでもネットワークにつながる，いわゆるユビキタス情報化社会が進展する中で，センサネットワークが活用される場面がますます広がってきており，かつ，センサネットワークは大規模化してきている．たとえば，BEMS（Building and Energy Management System）[26] 等が大規模なセンサネットワークを活用した応用の例である．

大規模なセンサネットワークでは，サーバ側からつねにすべてのノードに一律に指示を出して制御することは効率面から現実的ではなく，ノードのグループを定義してグループ単位に管理することが必須になる．たとえば，ある建物の同じ階に設置されたグループに対して初期設定情報を送信したり，特定のセンシング機能を持つグループに対してコマンドを送信したりするような形態は，センサネットワークにおいてはきわめて日常的であり，多用される通信形態であるということができる．

大規模なセンサネットワーク上で安全なアプリケーションを構築・運用するためには，センサネットワークにおけるグループを安全に管理するためのグループ鍵管理が重要である．つまり，これらグループ通信の内容を暗号化する仕組みや，通信情報の改ざんや偽造を防ぐ仕組みの導入が必要となる．グループのメンバだけが知りうる「グループ鍵」を導入し，各種の暗号技術を使うことで上記の安全性を確保することが可能となるが，グループ鍵については，グループの実態に即した形でこれを管理する必要がある．特に大規模なセンサネットワークにおけるグループ鍵管理では，以下に述べる 2 つの点を十分に考慮する必要がある．

1 点目は，グループ化されたノードは，時間の経過に応じて変化する可能性がある点である．現実のセンサネットワークの応用では，新しいノードを参加させて既存のグループに追加したり，故障，紛失，あるいは盗難等の理由で，既存のノードがグループから離脱したり

†1 NEC サービスプラットフォーム研究所
Service Platforms Research Laboratories, NEC Corporation
†2 奈良先端科学技術大学院大学
Nara Institute of Science and Technology

する事態も起こりうる．グループから離脱するノードが発生した場合でも安全性を継続して確保するためには，離脱ノードの保有する鍵情報が悪用されないよう対策する必要があるが，ノードの紛失・盗難等の理由で離脱ノードの制御が不可能となる事態を想定すると，速やかにグループ鍵を更新し，離脱ノード以外のグループメンバに新しいグループ鍵を再配送すること（ノード無効化）が事実上唯一の解決法となる．グループに所属するメンバ数が少ない場合，離脱ノード以外に対してユニキャスト的に新しいグループ鍵を配送することも可能であるが，中・大規模グループにおいてユニキャスト的な鍵配送を行うことは，効率面から問題がある．大規模グループにおいて効率的にグループ鍵を更新する方式は，情報セキュリティの分野で多く研究されており，たとえば鍵管理情報を木構造に基づいて定義する方式等がよく知られている[15)]．

注意すべき 2 点目は，1 台のノードが，複数のグループに同時に所属する可能性がある点である．たとえば，1 台のノードが「3 階に設置されたノードのグループ」「温度センサを持つノードのグループ」に同時に属する，という形態をあらかじめ想定する必要がある．これに対する安直な解決法は，上述したようなグループ鍵管理方式を複数独立して導入することであるが，この安直な方式では，鍵記憶のためのメモリ量や鍵管理の通信負荷が，所属するグループ数に応じて増加してしまう．これは，資源が非常に限定されたノードでは，致命的な問題となることも考えられる．文献 19) では，グループ鍵管理のための木構造を独立して定義するのではなく一部の部分木を共通化することで，鍵個数の削減を検討している．1 個の情報が複数のグループ鍵管理に貢献するという意味で興味深い点もあるが，木構造を再構築するときまで離脱ノードがグループ鍵を保持することを許す等，ノード離脱に関する問題を本質的に解決していないという意味で，実用的な解決法にはなっていない．

本研究では，上記 2 つの観点に十分留意して，大規模センサネットワークにおけるグループ鍵管理方式を提案する．具体的には，上記 2 つの観点に基づき，次のような 4 つの要件を満たすようなグループ鍵管理方式を設計する．

要件 1　任意のタイミングでグループ鍵の更新が可能である．
- 第 1 の観点から，グループの動的な変化に追随してグループ鍵の更新を実施できるべきである．

要件 2　大規模なグループを効率的に管理できる．
- 大規模なセンサネットワークでは，個々のグループの規模も大きくなるので，そのような場合でも実用的な処理効率を確保できるべきである．

要件 3　1 台のノードが複数グループに属するときの負荷増が緩やかである．
- 第 2 の観点から，1 台のノードが複数グループに同時に所属しても，実用的な処理効率を確保できるべきである．

要件 4　サービス内容から導かれる自然な属性に基づいてグループを定義できる．
- サービスにとって有益なグループを管理できるべきである．

以降では，2 章で関連研究について，本研究の位置づけとともに説明し，3 章で提案方式を説明する．さらに 4 章では，典型的な応用として BEMS を設定し，提案方式と既存方式の比較評価を行う．最後に 5 章でまとめる．

2. 関 連 研 究

2.1 既存方式の分類

本研究はセンサネットワークにおける鍵管理方式の研究という範疇に入る．そのなかでも特に本研究はグループ鍵管理方式を対象とするが，本研究の位置付け・アプローチを明確化するため，本節ではセンサネットワークにおける鍵管理方式に関する既存方式の分類・整理を試みる．センサネットワークで頻出する無線通信では，特定のノードに限定して鍵情報を送り届けることが困難であるため，暗号技術を用いて，通信路上の情報を入手したとしても，そこから有用な情報を第 3 者に漏洩させないことが求められる．暗号技術に基づいた鍵管理方式として，公開鍵暗号に基づく鍵管理方式，すなわち，文献 24) に代表されるような数論的な手法を利用する方式が知られている．しかし，それらの方式はセンサネットワークに適用するうえでは，資源制約の厳しいノードに大規模な計算を課す必要が生じるという問題がある．したがって，センサネットワークを対象とした本研究および以下に説明する既存方式では，現実的な方式として，対称鍵暗号や 1 方向ハッシュ関数等の軽量な処理のみで完結するシンプルな方式を採用している．

センサネットワークにおける鍵管理方式については，2 つの異なる分類軸を導入し，各分類軸について，それぞれ 2 つの管理モデルを定義することができる．1 つ目の分類軸は，管理対象となる鍵の機能に着目するものであり，ノード間の秘匿通信のために，ノードペアごとに共有されるペアワイズ鍵の管理モデル，グループでの秘匿通信のためにグループに属するノード全員で共有されるグループ鍵の管理モデルの 2 種類が考えられる．もう 1 つの分類軸は鍵管理を実現する仕組みに着目するものであり，鍵の更新時に，信頼できる鍵管理者（サーバ）の存在を仮定する中央管理型モデル，当該ノードだけで鍵更新を完了することのできる自律型モデルの 2 種類が考えられる．上記分類軸に従って，既存研究を分類すると，**表 1** のようになる．

表 1　センサネットワーク向け鍵管理方式の分類
Table 1　A classification of key management schemes for sensor networks.

管理対象	中央管理型	自律型
ペアワイズ鍵	文献 1)，2)	文献 3)–12)
グループ鍵	文献 13)–19)	文献 20)–23)

ペアワイズ鍵管理–中央管理型モデルとして，文献 1)，2) がある．文献 1)，2) は各ノードがサーバとの間で 1 対 1 に保持するマスタ鍵を使って，ペアワイズ鍵を送受信ノードに個別配送する．

ペアワイズ鍵管理–自律型モデルとして，文献 3)–12) がある．これらの方式では，ペアワイズ鍵を生成するための情報（鍵種）をノードに事前格納することで，アドホックに通信を開始するノード間でのペアワイズ鍵共有をローカルに実現する．鍵種の選択のため，ノードの部分集合（ある種のグループ）を想定する研究[10] もあるが，後述するグループ鍵管理モデルと混同しないように注意する必要がある．

グループ鍵管理–中央管理型モデルにおける単純な方式 13)，14) では，各ノードがサーバとの間で 1 対 1 に保持するマスタ鍵を用い，サーバがグループ鍵をグループ内のノードに個別に配送する．文献 15)–17) は，グループごとに定義する木構造を利用してグループ鍵を配送する．文献 18) は，1 方向性ハッシュ関数とグループごとに定義する木構造を利用してグループ鍵を配送する．文献 19) は，グループ鍵管理のための木構造を独立して定義するのではなく一部の部分木を共通化することで，鍵個数の削減を検討している．

グループ鍵管理–自律型モデルの例として，文献 20)–23) がある．文献 20) は，後述するような特殊なハードウェア上の仕組みを導入し，グループ鍵を含む暗号鍵管理を行う．文献 21)，22) は，サーバとの通信が切断されても各ノードがローカルな計算のもとでグループ鍵を更新する仕組みを提示している．文献 23) は，サーバの代理者をグループ単位に設け，代理者を介して個々のグループ鍵を更新する．

2.2　本研究の位置づけ

本研究ではグループ鍵管理–中央管理型モデルを採用する．任意のノードとノードとの間の鍵共有は表 1 の分類でいうペアワイズ鍵の管理に相当し，本研究の枠組みで対象としない問題である．グループ鍵を管理するにあたって，機能的には，自律型モデルのほうが中央管理型モデルよりも優れている部分もある．しかし，自律型モデルでは本来サーバが行う機能を複数ノードが分担して行うことになるため，方式が複雑・非効率になったり，追加の前提条件が必要となったりする傾向がある．ノードが動的に動き回るアドホックな応用等では自律型モデルを採用せざるをえない場面もあるが，4 章で述べる BEMS のように，ノードが静的に設置され，サーバとの接続性が確保されるような応用では，中央管理型モデルのほうが実用性が高いといえる．グループ鍵管理–中央管理型モデルの枠内でも様々な機能を持った方式が検討できるが，本研究では，前章で述べた 4 つの要件を満たす方式の実現を目的とする．以降では，これら要件を基準として，グループ鍵管理–中央管理型モデルの方式を比較する．

文献 13)，14) の方式では，各ノードとサーバとの間でユニークな（ノードごとに異なる）マスタ鍵が共有されていることを前提としている．あるノードがグループから脱退する際には，グループ鍵の更新が必要になるが，このとき，脱退するノード以外のすべてのグループ内ノードに対し，（新しい）グループ鍵をそのノードのマスタ鍵で暗号化して送信することを繰り返す．この方式では，グループ鍵配送にかかる通信負荷がグループ内のメンバ数に対して 線形オーダ で増加するため，多数のメンバを有する大規模グループでの鍵管理において，要件 2 を満たせないおそれがある．

大規模なグループにおける効率的なグループ鍵管理を実現する手法としては，文献 15) が広く知られている．文献 15) では，鍵木と呼ぶ木構造を利用してグループ鍵配送にかかる通信回数を削減する．鍵木の各頂点には暗号鍵が割り当てられており，また，葉頂点とノード（ユーザ）との間に 1 対 1 の対応関係が定義されている．各ノードには，対応する葉頂点の先祖頂点に割り当てられた暗号鍵を事前に配送しておくものとする．すべてのノードは鍵木の根頂点の鍵を共有するので，この根頂点の鍵をグループ鍵として利用する．あるノードがグループから脱退する際には，脱退ノードの持つ暗号鍵をすべて無効化する必要がある．具体的には，無効化された鍵を置き換える新しい鍵を，それを保持すべきすべてのノードに配送する．このとき，鍵木に沿ってボトムアップ的に新しい鍵を配送することにより，全ノード数に対して 対数オーダ の手間で，ノード無効化処理を実現することができる．基本的に文献 15) は，1 個のグループに対する鍵管理手法であるが，副次的に，鍵木の中間節点に対応するノード部分集合という「別のグループ」を想定することが可能である．たとえば，文献 15) の鍵木に基づき，位置的に近接するノード集合をグループと見なす文献 16)，通信頻度の高いノード集合をグループと見なす文献 17) が存在する．しかし，これら副次的なグループは，サービス実現において有用なグループ形態とは一致しないことがあり，要件 4 を満たせない．複数のグループを柔軟に設定したい場合，これらの方式では 1 台のノードが独立した複数グループに加入することは考慮されていないため，鍵木を複数独立して導入する必要があり，要件 3 を満たすことができない．文献 18) は文献 15) の改良

表 2　グループ鍵管理–中央管理型モデルの方式比較
Table 2　A comparison of centrally-managed group key management schemes.

方式	要件 1	要件 2	要件 3	要件 4
文献 13),14)	○	×	○	○
文献 15),18)	○	○	×	○
文献 16),17)	○	○	×	×
文献 19)	×	○	○	○
提案方式	○	○	○	○

方式であり，ノード無効化処理における通信負荷を文献 15) より削減可能であるが，要件 3 への対応において，本質的に文献 15) と同じ問題がある．

文献 19) は，ユーザが同時に複数のグループに所属するようなケースを考え，鍵木の一部を共用化する方式について議論している．文献 19) では，複数の鍵木が，その部分木を一部共用するような仕組みを提案している．1 個の情報が複数のグループ鍵管理に関与するため，情報の効率利用という意味では，センサネットワークでの利用に向いた方式である．致命的な問題は，ノードの新規追加やグループからのノード離脱等の操作を間欠的にしか実現できていない点にある．特に，安全運用においては，脆弱性の疑われるノードを可能な限り迅速に無効化することが求められるが，文献 19) では，離脱ノードが長期にわたって（次に鍵木を再構築するまで）グループ鍵を保持することを許容しているため，要件 1 を満たす方式とはいい難く，高い機密性の要求される応用での利用は難しいといえる．

以上を整理するとグループ鍵管理–中央管理型モデルについて，既存方式と提案方式における各要件への対応は**表 2** のように整理される．4 つの要件をすべて満たす既存方式はなく，提案方式ではこれら 4 つの要件を満たすことを目的としている．定量的な評価が必要な要件 2，3 に関しては，4 章で詳細に議論する．

グループ鍵管理–自律型モデルの既存方式を中央管理型のモデルに適用することももちろん可能である．しかしながら上述のとおり，自律型のモデルはサーバレスで管理可能という利点を得られる反面，実現性や効率の観点で欠点がある．たとえば，特殊なハードウェア上の仕組みを導入することで，グループ鍵を含む暗号鍵管理を効率的に行おうとの試みが文献 20) で提案されている．文献 20) では，すべてのノードは外部から操作できない時計を内蔵しており，特定時刻を過ぎると，ノード内部の機密情報を完全かつ確実に消去することが求められる．もし，ノード故障等の理由により機密情報の消去に失敗したり，あるいは，機密情報消去までにノードが盗難・内部解析されたりした場合，そのノードだけでなく，応用システム全体の安全性が保証されなくなってしまう．文献 20) を安全に利用するためには，低コストで大量生産されるノードについて十分な動作信頼性を保証する必要があるが，それが現実的であるかどうかは，議論の分かれるところである．文献 21)，22) は，ネットワークの全稼働時間を有限のセッションに分割することで，あるセッションにおけるグループ鍵をローカルに計算可能とする．鍵更新のたびにセッションを消費していくため，システム全体としての稼働時間が制限されることになる．現実のシステムでは，一部のノードを交換しつつ，永続的にシステムを維持することも一般的と考えられるが，そのような運用も行えなくなる．また，文献 21)，22) では，鍵のメモリ負荷および更新に要する通信負荷において，巨大素数の対数オーダを要し，上記の中央管理型モデルの方式，たとえば文献 15) 等に比較して効率的ではない．文献 23) では，各グループにクラスタヘッドと呼ぶサーバの代理者を設け，クラスタヘッドが当該グループの鍵更新を担う．各ノードは同じグループのクラスタヘッドに接続できればよいため，鍵管理の自律性は完全な中央管理型モデルに比べ高いと考えられるが，各グループにおいて鍵更新にかかる通信負荷がグループ内のメンバ数に比例し，文献 13)，14) と同程度に要件 2 への対応が困難である．

また，ペアワイズ鍵管理モデルでも，マスタ鍵の代わりにノード間で共有するペアワイズ鍵を使用することで，文献 13)，14) に類するグループ鍵管理を実現できる．しかし文献 13)，14) と同様に，要件 2 を満たせない．

3. 提 案 方 式

本研究では，センサネットワークの応用において，任意のグループ構造が独立して存在するのではなく，ノードの持つ「属性値」により自然に定義されるグループが複数存在することを想定し，1 台のノードが自然に加入することになる複数グループを想定したグループ鍵管理方法を検討する．以下 3.1 節では，想定しているネットワーク環境と，提案方式を実現するための前提条件について述べる．3.2 節，3.3 節では，本研究で考えるグループの構造について検討し，その形式化を行う．特に 3.3 節では提案方式において重要な条件について説明する．3.4 節では，3.2 節，3.3 節で与えるグループ構造の下で安全かつ効率良くグループ鍵を更新するためのプロトコルを示す．

3.1　想定するネットワークと前提条件

本論文では，複数のノードと 1 台のサーバからなるセンサネットワークを考え，文献 15), 18) と同様に，サーバから全ノードに対して放送型配信の可能なネットワークトポロジを想定する．放送型配信が可能であればよく，たとえばサーバを中心とするスター型への適用が可能である．本章では議論の汎用性を確保するために，トポロジを特定せずに議論を行う．

その後，4 章において，スター型トポロジを対象に提案方式が機能することを定量的に示す．

サーバは汎用の計算機であり，十分安全な管理体制下で運用されるものとする．すなわち，サーバから機密情報が漏えいしたり，サーバが不正行為を行うことは想定しない．これに対し，ノードについては「比較的弱い耐タンパ性を持つ記憶領域」を備え，「比較的弱い管理体制」の下で運用されることを想定する．具体的には，以下の条件が成立することを仮定する．

- ノードの内部情報が不正な解析行為によって露呈することは完璧には防げないが，ノード内部情報の参照や改変には一定の時間がかかる．
- ノードの盗難を完全に防ぐことは困難であるが，一定の盗難抑止措置が講じられており，複数のノードが同時に攻撃者に入手されることはない．また，ノードの盗難が発生した場合は，ただちにその旨がサーバに通報される．

軍事用途等を含めたすべてのセンサネットワークの応用で上記条件を達成できる保証はないが，この条件が比較的妥当な応用は多いと考えられる．たとえば，SD カード[25] 等の低コストで実用的な耐タンパ性能を提供するシステム LSI を利用可能な状況が多くなっていることや，本論文 4 章でオフィスビルの省エネルギー化のためにセンサネットワークを利用する例を想定して議論を行うように，運用上の前提として，オフィスビルへの入退室は厳重に管理されること，ビル内は多くの利用者やビデオカメラ等により衆人環視状態にあること，固定用ワイヤや振動検知アラーム等でノードに対する物理的な攻撃を抑止できること等をふまえると，上述の条件は，かなりの程度で達成されると考えることができる．

提案方式は，上述のような環境において，脆弱性の疑われるノード内部の情報が不正利用される前に，速やかに当該ノードを無効化する手段を提供する．上記の条件が成立しない場合，提案方式では安全性が確保できなくなる場合もある．この問題については，4.4 節であらためて議論を行う．

3.2　ノードの属性から定義されるグループ構造について

多くの実用的なセンサネットワークの応用においては，何らかの「属性」に着目して各ノードを特徴づけ，同じ属性値を持つノードをグループ化して取り扱う機会が多いと考えられる．たとえば，ノードの設置方角という「属性」を考え，各ノードは東，西，南，北のうち 1 つの属性値を持つものとすると，「東（西，南，北）の方角に設置したノードの集合」が概念的に定義されることになる．あるいは，設置フロアという別の「属性」を考えることで，たとえば「3 階に設置されたノードの集合」が定義され，さらに「高次」の集合として，「3 階の東側に設置されたノードの集合」が導かれることになる．このように，ノードの持つ属性値によりノードをグループ化することはきわめて自然であり，このように定義されたグループは，センサネットワークの応用においても，一定の意味を持つことが期待でき，要件 4 への対応を現実的なものとする．本研究では，上述のように定義されるグループにおけるグループ鍵について検討を行う．

グループ鍵は，グループに属するノードとサーバだけが知る秘密情報である．グループ鍵と暗号技術を用いることで，グループメンバだけに限定した同報通信等を実現することが可能となる．上述のとおり，本研究で考えるグループは，センサネットワーク運用上意味のある集合となっているため，これに対してグループ鍵を与えることは，安全で信頼できるアプリケーション構築に貢献すると考えられる．

属性および属性値については，センサネットワークがどのような環境でどのような目的に使われるかで，大きく異なってくると考えられる．上述のように，設置場所に関する情報を属性値とすることは多くの局面で有効と考えられるが，たとえば，1 つのネットワークの中に温度センサ，人感センサ等，異なるセンシング機能を持つノードが含まれる場合には，「搭載センサ機能」という属性が必要になるであろう．あるいは，複数の事業者の設置したノードの通信下位レイヤを相互接続し，1 個の密なセンサネットワークを構成するような場合においては，各ノードには「事業者」という属性が紐付けられると考えられる．何種類の属性を考えるか，何を属性とするか，各属性に対してどのような属性値を定義するかは，ネットワークの設計・運用にあたっては課題となるが，本研究では，属性および属性値は事前に決定され，外部から与えられるものとして議論を行う．ただし，すべてのノードは，定義されたすべての属性について，ちょうど 1 個の属性値を持つことを前提条件として仮定する．「特定の属性値が定義されていない」，「複数の属性値が定義されている」ことを想定しない，との仮定であるが，たとえば「未定義」という属性値を新たに設定する等，運用上の対応によって，本仮定は容易に達成することができると考えられる．

N を，ノード全体からなる集合とする（サーバは N には含まれない）．集合族 $A = \{G_1, G_2, \ldots, G_m\}$ が以下の条件を満たすとき，A を N の**分割**という：

- $G_i \subset N$
- $i \neq j$ ならば $G_i \cap G_j$ は空集合である
- $G_1 \cup G_2 \cup \cdots \cup G_m = N$

いま，対象とするセンサネットワークにおいて d 個の属性を定義し，i（$i \leq d$）番目の属性には m_i 種類の属性値を定義することを考える．このとき，「i 番目の属性については j 番目の属性値をとる」ようなノードの集合を $G_{i,j}$ と書くことにすると，上述の属性値

に関する一意性の仮定より，$A_i = \{G_{i,1}, G_{i,2}, \ldots, G_{i,m_i}\}$ は N の分割となる．本論文では，ノード集合 $G_{i,j}$（$1 \leq i \leq d, 1 \leq j \leq m_i$）をノードの**一次グループ**と呼び，一般に，$G = G_{i_1,j_1} \cap G_{i_2,j_2} \cap \cdots \cap G_{i_k,j_k}$ として与えられるノード集合 G を k **次グループ**と呼ぶ．ただし，$1 \leq k \leq d$ であり，$i_1, i_2, \ldots, i_k$ は 1 以上 d 以下の相異なる整数，$1 \leq j_a \leq m_a$（$1 \leq a \leq k$）とする．次数について意識する必要がない場合，G を単にグループと呼ぶ．以上の定義より明らかなとおり，本論文では，いくつかの属性値が共通するようなノードの集合をグループと呼称する．一般に，センサネットワークの応用の中には多数のグループが存在し，ノードは，その属性値に従い，複数のグループに所属することとなる．d 次グループは，集合の包含関係に関して極小のグループである．

3.3　グループ構造における条件

3.2 節で述べたグループ構造に対して，満たすべき条件を以下に示す．これは 3.4.2 項の前方安全性を考慮するうえで重要な条件となる．

条件 1　任意の d 次グループについて，その要素数はたかだか 1 である．

すなわち，任意の $(1, j_1), (2, j_2), \ldots, (d, j_d)$ について $G = G_{1,j_1} \cap G_{2,j_2} \cap \cdots \cap G_{d,j_d}$ が空集合となることは許すが，G が 2 個以上のノードを含むことはないと仮定する．自然に導かれる属性を使用しただけでは，本条件を満足できない場合もあると考えられるが，「d 次グループ内でのシーケンス番号」に相当する人工的な属性を 1 個追加すれば，上記条件を達成することができる．

図 1 は，提案方式におけるグループ構造を説明する図である．たとえば，単一のセンサを搭載するノードが複数の設置フロアに点在する場合，「搭載センサ機能」および「設置フロア」という属性に着目でき，各々において一次グループ G_{1,j_1}，G_{2,j_2} を考えることができる．これらの集合の包含関係によって 2 次グループが定まる．ただし，同一のフロアに同じセンサを搭載するノードがたかだか 1 つであるとは限らない場合，条件 1 を満たすために，$G_{1,j_1} \cap G_{2,j_2}$ におけるグループ内でのシーケンス番号に相当する人工的な属性 G_{3,j_3} を追加する必要がある．このとき，一次グループ G_{3,j_3} は，$G = G_{1,j_1} \cap G_{2,j_2}$ において，同じシーケンス番号を与えられるノードの集合となる．3 次グループ $G' = G_{1,j_1} \cap G_{2,j_2} \cap G_{3,j_3}$ において，要素数はたかだか 1 であり，条件 1 を満たす．図 1 において，各ノードは○で示されており，○内の数字は，ノードに与える人工的な属性であるシーケンス番号を示す．

ただし，d 次グループに収容されるノードが非常に多かった場合に，d 次グループ内でのシーケンス番号に相当する属性をただ 1 個追加しただけでは必ずしも効率的とはならない．その場合は，以下のような拡張を与えてもよい．d 次グループにおける最大のノード数以上の葉数を持つ完全 n 分木を用意し，葉に d 次グループ内のノードを配置する．そして，根頂点から葉に至るまでの各階層において「何番目の節を経るか」に相当する人工的な属性を複数追加する．本拡張によって，追加する属性値数を，d 次グループに収容される最大ノード数の対数オーダに抑えられる．図 1 と同様に一次グループ G_{1,j_1}，G_{2,j_2} のみが存在するとき，これらの集合の包含関係によって 2 次グループが定まる．2 次グループにおける最大のノード数が 8 のとき，**図 2** のように高さ 3 の完全 2 分木を与え，葉に 2 次グループ内のノードを配置している．3 つの階層において，それぞれに「何番目の節を経る

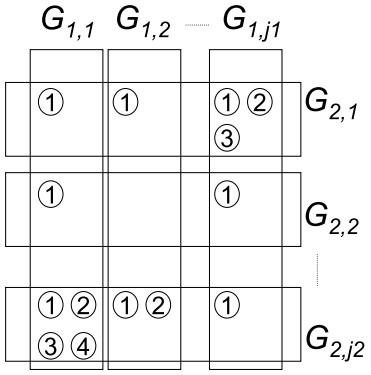

図 1　グループ構造の例
Fig. 1　An example for group structure.

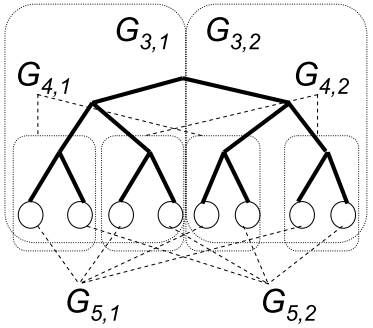

図 2　人工的な属性の拡張
Fig. 2　An extended artificial attributes.

か」に相当する人工的な属性 G_{3,j_3}，G_{4,j_4}，G_{5,j_5} を追加している．このとき，5 次グループ $G = G_{1,j_1} \cap G_{2,j_2} \cap G_{3,j_3} \cap G_{4,j_4} \cap G_{5,j_5}$ において，要素数はたかだか 1 であり，条件 1 を満たす．以下の議論では，この条件が満足するよう属性および属性値が定められていることを前提として議論を行う．

3.4　グループ鍵の管理方式について

3.4.1　グループ鍵の定義と初期化

センサネットワークの中には，前節で定義されたようなグループが多数存在する．それぞれのグループに対して個別に独立したグループ鍵を定義すると，1 台のノードは，自らの所属するグループ数に比例した個数のグループ鍵を管理する必要が生じるため，大きな記憶領域が消費されてしまうことになる．この問題を避けるため，一次グループに対してのみ独立したグループ鍵を定義し，二次以上のグループに対しては，一次グループのグループ鍵を組み合わせてグループ鍵を構成することを考える．一次グループに対してのみ独立して定義するグループ鍵を**要素鍵**と呼ぶ．サーバは，すべての一次グループ $G_{i,j}$（$1 \le i \le d$，$1 \le j \le m_i$）に対し，要素鍵 $k_{i,j}$ をランダムかつ独立に決定する．次に，一次グループ $G_{i,j}$ に属するすべてのノードに要素鍵 $k_{i,j}$ および要素鍵の発行時刻を運用に先立って事前に格納する．もしくは安全な通信路を仮定してそのうえで配送する．d 種類の属性が存在するため，1 台のノードは，全部で d 個の要素鍵（およびその発行時刻）を保持することになる．グループ鍵はこれらの要素鍵から以下のように計算される．グループ G が，$G = G_{i_1,j_1} \cap G_{i_2,j_2} \cap \cdots \cap G_{i_k,j_k}$ として定義されるものとする．このとき $k(G) = h(k_{i_1,j_1} || k_{i_2,j_2} || \cdots || k_{i_k,j_k})$ と定義し，これを G の**グループ鍵**と呼ぶ．ここで h は事前に選んでおいた 1 方向性ハッシュ関数であり，$||$ は連接演算子を表す．グループ鍵 $k(G)$ を計算するためには，要素鍵 $k_{i_1,j_1}, k_{i_2,j_2}, \ldots, k_{i_k,j_k}$ をすべて知っている必要がある．したがって，$k(G)$ を計算することができるのは，グループ G に属するノードのみとなる．

3.4.2　ノード無効化を考慮したグループ鍵の更新

センサネットワークに特有の脅威としてノードの盗難がある．盗難ノード内部の暗号鍵等が不正者の手に渡ると，機密情報の漏えいや通信データの偽造等が行われる可能性があるため，ノードの盗難が発覚した場合は，速やかに当該ノードの無効化を行う必要がある．盗難に遭ったノードは管理者の制御下から離れている可能性が高いため，機密情報を消去するようなコマンドを管理者が盗難ノードに向けて発信したとしても，ノードがコマンドを受信して正常に動作することは期待できない．この問題を回避するには，盗難ノードが所有するすべての鍵の使用を停止し，盗難ノード以外のすべての（権限ある）ノードに対して新しい鍵を配送する必要がある．この際，古い鍵で新しい鍵を暗号化する手法は利用できない．なぜなら，ノードを盗んだ攻撃者が通信路上の暗号文を記録・保存しておき，盗難ノード内部から暗号鍵を抽出した後に，暗号文の解読を行う可能性もあるためである．いわゆる前方安全性を確保するためには，盗難ノードが持つ鍵をいっさい使わずに，安全かつ効率的に新しい鍵の配送を行う必要がある．

提案方式では，1 台のノードは各属性に対応して要素鍵を持つため，盗難ノードの内部には d 個の要素鍵が格納されている．盗難ノードを n とし，n に格納されている d 個の要素鍵を $k_{1,j_1}, k_{2,j_2}, \ldots, k_{d,j_d}$ とする．ノード n を無効化するには，これら d 個の要素鍵の使用を停止し，G_{i,j_i}（$1 \le i \le d$）の新しい要素鍵 k'_{i,j_i} をノード集合 $G_{i,j_i} \setminus \{n\}$ に配送する必要がある．これを安全かつ効率的に実現するため，以下のプロトコルでは，「ソルト」と呼ばれる情報を n 以外のノードに配送し，古い要素鍵とソルトから新しい要素鍵を導出することを考える．この手順は，具体的には以下のプロトコルにより与えられる．ここで $E_k(x)$ は情報 x を鍵 k で対称鍵暗号アルゴリズムにより暗号化して得られる暗号文であり，$\langle \cdot \rangle$ は，括弧内の情報から構成される更新用データを表す．

(1)　サーバは，**ソルト**と呼ばれるランダムな情報 S を決定する．また，新しい要素鍵の発行時刻 t を決定する．

(2)　サーバは，n 以外のノード全体からなる集合を U とする．

(3)　サーバは，U が空集合になるまで以下を繰り返す．

(a)　$G_{i,j} \cap U \neq \emptyset$，$n \notin G_{i,j}$ となる一次グループ $G_{i,j}$ を 1 つ定め，$x_{i,j} = E_{k_{i,j}}(S, t, (1, j_1), (2, j_2), \ldots, (d, j_d))$ を計算する．

(b)　$\langle i, j, x_{i,j} \rangle$ を $G_{i,j}$ に向けて同報送信する．

(c)　$U \leftarrow U \setminus G_{i,j}$ とする．

(4)　$\langle i, j, x_{i,j} \rangle$ を受信したノードは，自分が $G_{i,j}$ に属さない場合これを棄却する．自分が $G_{i,j}$ に属する場合，以下を実行する．

(a)　$x_{i,j}$ を復号し，S，t および $(l, j_l)(1 \le l \le d)$ を入手する．

(b)　自分の持つ要素鍵の中に無効化される要素鍵 k_{l,j_l} があり，k_{l,j_l} の更新時刻が t よりも古いとき，$k'_{l,j_l} = h(S || k_{l,j_l})$ を計算して G_{l,j_l} の新しい要素鍵とし，この要素鍵の発行時刻を t に更新する．

無効化される要素鍵 $k_{1,j_1}, k_{2,j_2}, \ldots, k_{d,j_d}$ の更新には，古い要素鍵とソルト S が必要となる．サーバは，上記ステップ (3) において，n を含まない一次グループのみを用いて n 以外のすべてのノードを被覆する集合族を求め，各一次グループの要素鍵を用いて S を暗号

化する．n はいずれの一次グループの要素鍵も持たないため，暗号化された S を復号，入手できず，また，n 以外のすべてのノードは少なくとも 1 個の暗号文を復号できるため，S を知ることができる．これにより，無効化ノード n 以外のすべてのノードに S を配送することが可能となり，安全に要素鍵を更新することができる．本プロトコルを実施するにあたって，文献 19) のようなタイミング的な制約はなく，運用中における任意の時点で実施可能である点で，要件 1 を満たすプロトコルということができる．

上記手順の負荷は，n 以外のノードを被覆する集合族の要素数に比例する．要素数が最小の被覆を求めることは，NP 困難である集合被覆問題の変形と考えられるため，厳密な最適解を効率的に求めることは難しいと考えられるが，最悪の場合であっても $G_{1,j_1},\ldots,G_{d,j_d}$ 以外の $\sum_{i=1}^{d}(m_i-1)$ 個の一次グループを利用すれば，求める集合被覆を構成することができる．したがって，本手順におけるサーバの暗号化操作実行回数および送信データ数は，たかだか $\sum_{i=1}^{d}(m_i-1)$ であるといえる．ノードは，自分の復号できるデータを 1 個だけ復号すればよいため，1 回の復号操作と，自らが所有する要素鍵のなかで更新の必要なものの個数と同じ回数のハッシュ値計算により，必要な要素鍵更新を完了することができる．また，発行時刻 t を利用することで，複数経路を通過して同一ノードに複数の同じ更新用データが到着しても混乱なく実行できる．また，攻撃者のリプレイ攻撃により混乱を生じることもない．

なお，盗難ノードが存在しない，つまり $\{n\}=\emptyset$ として同様の手順を踏むことで，単純にすべてのグループ鍵を更新することも可能である．このとき，サーバの暗号化操作実行回数および送信データ数は，たかだか $\sum_{i=1}^{d} m_i$ である．

3.4.3　ノードの追加

新しいノード n を，グループ $G_{i,j}$ に追加したい場合を考える．新しくグループに参加するノード n は，自分が参加する以前に $G_{i,j}$ のグループ鍵として使われていた鍵を知る権利はない．逆に，n をグループのメンバとして追加する過程において，n が以前のグループ鍵を知ることがあってはならない．この性質をグループ鍵における後方安全性と呼ぶ．後方安全性を有するノード追加プロトコルは，$G_{i,j}$ に以前から所属するノードには要素鍵 $k_{i,j}$ を用いて新しい要素鍵 $k'_{i,j}$ を知らせ，n に対しては個別に $k'_{i,j}$ を伝達すればよい．n に対する個別伝達については，初期化時と同様に，工場等で事前に格納するか，安全な通信路を仮定できる場合は，そのうえで配送する．本プロトコルにおいて，サーバにおける暗号化操作と通信の回数はたかだか 2 回，および既存ノードでの復号操作の回数はたかだか 1 回である．なお，n は，d 個のグループに同時に加入しなければならない．したがって本プロトコルを d 回繰り返し実行することで対応する．

4. 評　　価

4.1　想定する応用例

本章では，センサネットワークの有力な応用対象である BEMS[26] を例題とし，実用規模のアプリケーションに提案方式を適用した場合の効果について評価する．BEMS とはビル管理システムであり，ビルの機器・設備等の使用エネルギーや室内環境を把握し，これを省エネルギーに役立てるためのシステムである．ここでは，電気使用量を検針する機能を備えるノードと室内の温度，照度，湿度，人の在不在をセンシングする機能をそれぞれ有するノード，計 5 種類のノードをビル内の複数箇所に設置することを考える．センシング情報を収集する際には，サーバ（検針者）は対象のノードに対して，情報要求のための指令を発行する．指令を受けたノードは，センシングした結果をサーバに送り返す．サーバからノードへのダウンストリームは 1 対多，ノードからサーバへのアップストリームは 1 対 1 の通信となり，ともにセンサネットワークで頻出する通信形態である．本論文では，1 台のノードとの通信もメンバ数が 1 のグループとの通信と考えるので，1 対 1 の通信の部分についても提案方式を適用可能である．

ネットワークの規模としては，BEMS の需要が高い高層ビルを想定する．具体例として，40 階建のビル 2 棟（A，B 棟），各階には東西南北にフロアが存在するオフィスビルを想定し，各フロアに上記の 5 種のノードを設置し，BEMS を運用することを考える．このとき，サーバは以下のようなグループと通信するシナリオを考える．

- 同じ棟に存在するノード全体からなるグループ
- A 棟，B 棟を問わず，同じ階に存在するノード全体からなるグループ
- A 棟，B 棟，階数を問わず，同じ方角に存在するノード全体からなるグループ
- 設置場所を問わず同じ機能を有するノード全体からなるグループ
- ある棟の同じ階に存在するノード全体からなるグループ
- ある棟の同じ方角に存在するノード全体からなるグループ
- ある棟の同じ機能を有するノード全体からなるグループ
- ある階の同じ方角に存在するノード全体からなるグループ
- ある階の同じ機能を有するノード全体からなるグループ
- ある方角の同じ機能を有するノード全体からなるグループ
- 個々のノードからなるグループ

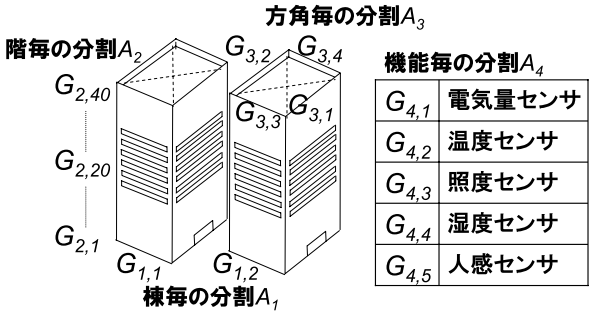

図 3　適用例における一次グループ
Fig. 3　Order-1 groups in our scenario.

表 3　通信する k 次グループ
Table 3　Order-k groups to communicate.

k 次グループ	グループ数	メンバ数
$G_{1,ji}$	2	800
$G_{2,j2}$	40	40
$G_{3,j3}$	4	400
$G_{4,j4}$	5	320
$G_{1,j1} \cap G_{2,j2}$	80	20
$G_{1,j1} \cap G_{3,j3}$	8	200
$G_{1,j1} \cap G_{4,j4}$	10	160
$G_{2,j2} \cap G_{3,j3}$	160	10
$G_{2,j2} \cap G_{4,j4}$	200	8
$G_{3,j3} \cap G_{4,j4}$	20	80
$G_{1,j1} \cap G_{2,j2} \cap G_{3,j3} \cap G_{4,j4}$	1,600	1

4.2　提案方式の適用について

以上のグループへの同報通信を実現するために，ノードを設置する棟，設置階数，設置方角，ノードの持つ機能のそれぞれをノードの持つ属性と考え，各属性ごとに分割 A_1，A_2，A_3，A_4 を考える．このとき，たとえば A 棟の 2 階の東にある温度センサを搭載したノードは唯一であり，提案方式の条件 1 を満たす．ここで各集合族のとりうる要素数は，ビル構造から $m_1 = 2$，$m_2 = 40$，$m_3 = 4$ となる．センサの種類に関しては将来の拡張を事前に想定し，$m_4 = 10$ とする．これにより最大で $2 \times 40 \times 4 \times 10 = 3{,}200$ ノードをネットワークに収容することが可能となる．想定では，各フロアに 5 種類のセンサを設置するので，1,600 ノードが実ノード数になる．このとき，適用例における一次グループは**図 3** に示すような構成となる．すなわち設置する棟に応じ $A_1 = \{G_{1,1}, G_{1,2}\}$，設置階数に応じ $A_2 = \{G_{2,1}, \ldots, G_{2,40}\}$，設置方角に応じ $A_3 = \{G_{3,1}, \ldots, G_{3,4}\}$，ノードの持つ機能に応じ $A_4 = \{G_{4,1}, \ldots, G_{4,10}\}$ の各集合族が定義され，グループは各集合族から選択する一次グループによって構造化される．四次グループにはたかだか 1 台のノードが存在するのみである．したがって，提案方式を適用するにあたっての条件 1 を満たす．**表 3** に，上記シナリオで通信するグループに対応する k 次グループを，そのグループ数および各グループのメンバ数とともに示す．

4.3　既存方式との比較

1 台のノードが表 3 に示す 11 個の各 k 次グループに同時に加入する想定環境のもと，提案方式と既存方式との比較を行う．なお，表 2 において，要件 1，4 を満たさない既存方式については，所定の機能を実現できないと考え，直接的な比較対象とはしない．要件 2，3 の観点で定量的に比較をするにあたって，ネットワーク全体でサーバが管理すべき鍵数とノードが記憶する鍵数についてまず議論する．次に，「鍵更新：月初めにすべてのグループ鍵を更新する」，「無効化：脆弱なノードをネットワークから切り離す」といった運用上十分に起こりうる鍵管理を想定し，それらに必要な通信負荷について議論する．提案方式は 3.1 節に示したとおり，放送型配信の可能なトポロジに適応することができる．比較においては，単純のため，既存方式を含め広く適応可能なスター型トポロジを想定して評価する．無線センサネットワークにおいて，サーバを中心とするスター型トポロジを構成する場合，サーバからの送信回数とノードの受信回数は等しくなり，これを比較することで，サーバ，ノード双方の通信負荷を評価できる．また有線センサネットワークにおけるバス型やリング型のトポロジ上に適用しても，同様の議論が可能である．

文献 13)，14) の場合，サーバで管理を要する鍵数はグループ数の総和と等しく 2,129 個となる．また，1 ノードあたりが記憶するグループ鍵数はノードが属しているグループ数と同数の 11 個である．すべてのグループ鍵を更新する際，これらの方式では，グループに対して古いグループ鍵で新しい鍵を暗号化して同報すればよいので，グループ数と同数の 2,129 回の通信が発生する．また，1 台のノードを無効化する際，無効化するノードを除いたグループに対し，マスタ鍵で新しいグループ鍵を個別に配送する必要があるので，$\sum_{g \in G}(|g| - 1) = 2{,}028$ 回の通信が発生する．ここで，G はある 1 台のノードが属するグループの集合を，$|g|$ はグループ g のメンバ数を示す．また，マスタ鍵は四次グループすなわちメンバ数が 1 のグループにおけるグループ鍵と同義と見なすことができる．

提案方式では，グループ鍵は属性値に紐づける要素鍵から計算できるため，管理の必要と

表 4　比較結果
Table 4　A comparison result.

方式	サーバの鍵数	ノードの鍵数	鍵更新負荷	無効化負荷
提案方式	56	4	56	52
文献 13)，14)	2,129	11	2,129	2,028
文献 15)	12,901	33	2,129	128
文献 18)	12,901	33	2,129	96

なる鍵の個数はサーバ側において属性値の総和 $\sum_{i=1}^{4} m_i = 56$ 個，ノード側においては属性数と同数の 4 個である．56 個の要素鍵を更新すれば全グループ鍵を更新することができるため，グループ鍵更新に必要なサーバの通信回数はたかだか $\sum_{i=1}^{4} m_i = 56$ 回である．また，1 台のノードを無効化する際，たかだか $\sum_{i=1}^{4}(m_i - 1) = 52$ 回の同報通信が発生する．

文献 15) によって，ノード無効化の際のグループ鍵配信を効率化することが可能である．文献 15) では実験的な評価により，分木数を 4 程度に設定した鍵木を利用することが，効率的であるという結果を示している．以降，鍵木を完全 4 分木で構成するとして評価する．このとき，ノードの無効化に必要な同報回数は鍵木の高さの 4 倍と見積もることができるので，考慮しているグループの場合，$\sum_{g \in G} 4 \log_4 |g| \approx 128$，すなわち約 128 回の同報で実現できる．ただし，文献 15) を適用するためには，管理用の鍵木を定義する必要があるため，管理する鍵数が増加することを忘れてはならない．鍵木の葉頂点に割り当てる鍵は，各ノードだけで構成するメンバ数 1 のグループのグループ鍵と同義であり，鍵木の根頂点に割り当てる鍵はグループに固有のグループ鍵であるので，実際には鍵木の中間頂点に割り当てる鍵を余分に持つ必要がある．このとき，サーバが管理する鍵数は，メンバ数が 1 以外のグループの集合を G' としたとき，$\sum_{g \in G'}(\sum_{k=1}^{\log_4 |g|-1} 4^k) = 10{,}772$ 個増加する．またノードの記憶する鍵数は $\sum_{g \in G}(\log_4 |g| - 1) \approx 22$，すなわち約 22 個増加する．さらに，文献 18) を使用すると，無効化時の同報回数は文献 15) の 3/4 の約 96 回と見積もることができ，ノードおよびサーバで記憶するべき鍵数もある程度の削減が可能である．ただし記憶しなければならない鍵数の上限値は文献 15) と変わらず，ノードの実装コスト削減にはそれほど大きくは貢献しない可能性もある．以上をまとめると鍵数および管理上の通信負荷の関係は**表 4** のようになる．なお表 4 において，提案方式で要する通信負荷と文献 18) で管理する鍵数は，必要とされる上限値を示す．

4.4 考　　察

提案方式は，1 台のノードが，表 3 に示す 11 個の各 k 次グループに同時に属するときに，既存方式と比べノードのメモリ負荷の 64%〜88%を削減できる．また，スター型トポロジを想定した場合においてサーバおよびノードの通信負荷の 46%〜97%を削減できる．センサネットワークでは，コスト上の問題から大容量の（特に耐タンパ性を有する）記憶領域をノードに確保することが困難であることが多いため，鍵のメモリ負荷を削減できる本方式は有効であると考えられる．さらに，通信負荷を削減できることは，電力資源を多用する通信回数を抑えられるという点で，電力資源の限られるノードの長期運用化を実現する．これらは汎用のネットワークに対しても好ましい性質であるが，これを対称鍵暗号の軽量な演算のみで実現できている点が最大の特徴であり，公開鍵暗号を用いずに実現できる点で，特にセンサネットワークに有用と考える．また，鍵更新処理のタイミングに制約を設けておらず，かつサービスに必要なグループを扱える点で要件 1，4 への対応も実現できており，文献 19) や文献 16)，17) に対する大きな利点と考える．通信負荷についてはスター型トポロジを想定した評価であるが，スター型のトポロジを構成するクラスタが親子関係を持つクラスタツリー型トポロジに適用する場合，クラスタヘッドと呼ばれるノード間で通信を中継することで通信の到達距離を長くすることが可能である．ただし，クラスタヘッドではリピータハブ的に受信したデータをそのまま転送する（再暗号化はしない）．このクラスタツリー型トポロジへの適用については，詳細には追加の条件を仮定して実験を行う必要があるものの，少なくともサーバ近辺のノードに関してはスター型と同様に受信負荷の軽減が期待される．さらに，クラスタツリーの各クラスタでも同等の効果が期待されるため，全体としての受信負荷の軽減につながると考えられる．予備的検討[27] においても，実ノードで構成するクラスタツリートポロジに対し，鍵更新の効率化を図れることも確認している．また，メッシュ型のネットワークトポロジにおいても，ルーティングテーブルの構築のためにブロードキャストが用いられることが多く，これを利用することでメッシュ型のトポロジ上に提案方式を適応できる可能性も考えられる．これらのトポロジにおいてはブロードキャストの効率性が性能に影響するため，ブロードキャスト効率化を実現する手法 28)，29) 等を用いたうえで提案方式を用いることが望ましい．

また，グループ鍵を動的に計算で導出する際のオーバヘッドについて考察する．提案方式では，表 4 に示したようにノードが静的に持つ鍵の数は削減されるが，そのつど 1 方向性ハッシュ関数を用いて動的にグループ鍵を計算するため，ノードの計算負荷は増加する．これに関して文献 14) に，ノードの必要とする電力の 98%が計算負荷からでなく，通信負

荷によるものであることが明記されている．文献 14) の計算は対称鍵暗号に基づいており，これは提案方式で用いる 1 方向性ハッシュ関数の計算コストと同等であることから提案方式に関しても同様のことがいえると考えられる．したがって，計算負荷の若干の増加はあるものの，通信負荷の削減効果が大きく得られる提案方式が，電力コストの大幅な削減を可能とする点でメリットが大きいと考えられる．

次にグループ構成の変化に関する感度について考察する．適用例では，収容できるノード数を 3,200 ノードまで考慮している．結果，グループ数は最大で 3,964 個に，1 グループあたりのメンバ数は平均で約 134 個増加する可能性がある．既存方式においては，管理すべき鍵数や通信負荷がグループ数または各グループのメンバ数に応じて増加するが，提案手法においては，表 4 に示す値から変わることはない．すなわち，提案手法は，システムの運用前において，そのスケールを十分に検討する必要があるが，スケールさえ適切に選ばれていれば，その範囲内において非常に良好なスケーラビリティを持つということができる．

最後に，提案方式の前提条件と安全性との関係について考察する．提案方式は要素鍵の組合せで高次グループのグループ鍵を導出するため，前提条件が満たされない場合，異なるノード内部の要素鍵の同時流出によって，高次のグループ鍵の安全性が損なわれる可能性がある．一方，本前提条件が満たされない場合，文献 15)，18) においても，鍵木の節点に紐つける鍵が複数漏洩し，それぞれで主張されているような安全性や効率性を確保することが困難になる．その意味で，提案方式と，文献 15)，18) との違いは，前提条件を明示的に扱うか（提案方式）暗黙のものとするか（文献 15)，18)）という性質のものであり，必要とする前提条件は共通である．文献 13)，14) との比較においては，前提条件は提案方式特有のものとなる．しかしながら，BEMS 等の応用を想定すると比較的自然に実現できるこれら条件を仮定できる場合は，提案方式がより効率的に作用するという点で一定の効果が認められると考えられる．したがって，提案方式の導入時には，これらの前提条件を達成するための運用上の仕組みをあわせて検討する必要がある．たとえば，加速度センサ等を使って，ノードが持ち出されたことをノード自身で警報するような運用技術[30] の導入等が有効と考えている．

5. おわりに

本研究では，ノードが自身の属性の組合せに応じて同時に複数のグループに加入する可能性が高い点に着目し，属性に紐づける管理情報を用いて複数のグループ鍵の管理の仕組みを互いに連携させ，複数グループのグループ鍵管理を効率化するグループ鍵管理方式を提案した．また，適用例を与え，既存方式と比べノードのメモリ負荷の 64%〜88%を，通信負荷の 46%〜97%を削減できることを示した．適用例においては，ノードの設置場所や機能を属性としてグループを構成することを検討したが，その他の属性を採用することも可能である．たとえば，応用に際して，効率的で有効な属性構造を構築することは重要であり，そのための指針を検討することは運用にあたっての今後の課題である．また，複数のトポロジを想定した実験により，ノードの通信負荷を詳細に評価することも興味深く，今後の検討課題とする．

参考文献

1) Neuman, B.C. and Ts'o, T.: Kerberos: An authentication service for computer networks, *IEEE Communications Magazine*, Vol.32, No.9, pp.33–38 (1994).
2) 阪田史郎（編著）：ZigBee センサネットワーク通信基盤とアプリケーション，pp.118–120, 秀和システム (2005).
3) Eschenauer, L. and Gligor, V.D.: A key-management scheme for distributed sensor networks, *Proc. 9th ACM Conference on Computer and Communications Security*, pp.41–47 (2002).
4) Chan, H., Perrig, A. and Song, D.: Random key predistribution schemes for sensor networks, *IEEE Symposium on Security and Privacy*, pp.197–213 (2003).
5) Chan, H. and Perrig, A.: PIKE: Peer intermediaries for key establishment in sensor networks, *Proc. IEEE INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp.524–535 (2005).
6) Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M.: Perfectly-secure key distribution for dynamic conferences, *Advances in Cryptology-CRYPTO'92*, pp.471–486 (1993).
7) Liu, D., Ning, P. and Li, R.: Establishing pairwise keys in distributed sensor networks, *ACM Trans. Information and System Security* (*TISSEC*), Vol.8, No.1, pp.41–77 (2005).
8) Blom, R.: An optimal class of symmetric key generation systems, *Advances in Cryptology: Proc. EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques*, Paris, France, April 1984, p.335 (1985).
9) Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J. and Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks, *ACM Trans. Information and System Security* (*TISSEC*), Vol.8, No.2, p.258 (2005).
10) Liu, D., Ning, P. and Du, W.: Group-based key predistribution for wireless sensor networks, *ACM Trans. Sensor Networks* (*TOSN*), Vol.4, No.2, pp.1–30 (2008).
11) Liu, D. and Ning, P.: Location-based pairwise key establishments for static sensor

networks, *Proc. 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp.72–82 (2003).
12) Jeong, J.M. and Haas, Z.J.: Predeployed secure key distribution mechanisms in sensor networks: Current state-of-the-art and a new approach using time information, *IEEE Wireless Communications*, Vol.15, No.4, pp.42–51 (2008).
13) Burmester, M.V.D. and Desmedt, Y.: A secure and efficient conference key distribution system, *Advances in Cryptology – EUROCRYPT'94*, pp.275–286 (1995).
14) Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E.: SPINS: Security protocols for sensor networks, *Wireless Networks*, Vol.8, No.5, pp.521–534 (2002).
15) Wong, C.K., Gouda, M. and Lam, S.S.: Secure group communications using key graphs, *Proc. ACM SIGCOMM'98 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication*, pp.68–79 (1998).
16) Lazos, L. and Poovendran, R.: Energy-aware secure multicast communication in ad-hoc networks using geographic location information, *IEEE International Conference on Acoustics Speech and Signal Processing*, Vol.4, pp.201–204 (2003).
17) Funayama, T., Imamura, S. and Okamoto, E.: Efficient Key Distribution System Using Communication Probability, *IPSJ SIG Notes*, Vol.2006, No.43, pp.1–6 (2006).
18) Sherman, A.T. and McGrew, D.A.: Key establishment in large dynamic groups using one-way function trees, *IEEE Trans. Softw. Eng.*, Vol.29, No.5, pp.444–458 (2003).
19) Jung, E., Liu, A.X. and Gouda, M.G.: Key bundles and parcels: Secure communication in many groups, *Computer Networks*, Vol.50, No.11, pp.1781–1798 (2006).
20) Zhu, S., Setia, S. and Jajodia, S.: LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks., *CCS'03*, *Proc. 10th ACM Conference on Computer and Communication Security*, pp.62–72 ACM Press, New York, (2003).
21) Liu, D., Ning, P. and Sun, K.: Efficient self-healing group key distribution with revocation capability, *Proc. 10th ACM Conference on Computer and Communications Security*, pp.231–240 (2003).
22) Dutta, R., Chang, E.C. and Mukhopadhyay, S.: Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains, *Applied Cryptography and Network Security*, Vol.4521, pp.385–400 (2007).
23) Guo, S., Shen, A.N. and Guo, M.: A Secure and Scalable Rekeying Mechanism for Hierarchical Wireless Sensor Networks, *IEICE Trans. Inf. Syst.*, Vol.93, No.3, pp.421–429 (2010).
24) Diffie, W. and Hellman, M.: New directions in cryptography, *IEEE Trans. Inf. Theory*, Vol.22, No.6, pp.644–654 (1976).
25) 岡田昌也，角　辰己，細川拓央：SD カードおよび IC カード用システム LSI，*Matsushita Technical Journal*, Vol.52, No.1, pp.104–109 (2006).
26) 下田　宏，大林史明：オフィスビルの省エネルギーとプロダクティビティ照明，電気学会論文誌 C（電子・情報・システム部門誌），Vol.128, No.1, pp.2–5 (2008).
27) 野田潤，楫　勇一，毛利寿志，仁野裕一，中尾敏康：複数の属性分割を利用したセンサネットワーク向け鍵管理方式の実装と評価，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム，pp.524–529 (2007).
28) 古川恭史，萬代雅希，渡辺　尚：指向性アンテナを利用した送信レート制御ブロードキャストについて，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2009）シンポジウム，pp.576–584 (2009).
29) 斎藤秀雄，田浦健次朗，近山　隆：適応スパニングツリーを用いた広域メッセージパッシングシステム用の集合通信（ネットワーク），情報処理学会論文誌コンピューティングシステム，Vol.46, No.12, pp.373–383 (2005).
30) 西原秀明，窪田裕介，村川友章，芳賀博英，金田重郎：焦電センサと RFID による室内向け物品位置検出手法，情報処理学会第 69 回全国大会，Vol.3, pp.279–280 (2007).

(平成 22 年 5 月 21 日受付)
(平成 22 年 12 月 1 日採録)

野田　　潤（正会員）

昭和 51 年生．平成 11 年大阪大学基礎工学部情報工学科卒業．平成 13 年同大学大学院修士課程修了．同年 NEC 入社，現在，NEC サービスプラットフォーム研究所ユビキタス基盤テクノロジーグループに所属．デジタル著作権管理，P2P の研究を経て，センサネットワーク，ネットワークセキュリティを中心としたユビキタスコンピューティングの研究に従事．

楫　　勇一（正会員）

平成 5 年大阪大学基礎工学部情報工学科卒業，平成 8 年同大学大学院修了．博士（工学）．同年 4 月より奈良先端科学技術大学院に勤務．この間，平成 15 年カリフォルニア大デービス校客員研究員，平成 16 年ハワイ大マノア校客員研究員．情報理論，情報セキュリティ基礎，オートマトン理論等に関する研究に従事．電子情報通信学会，情報理論とその応用学会，IEEE 各会員．

中尾　敏康（正会員）

昭和 43 年生．平成 5 年大阪大学大学院基礎工学研究科物理系情報工学専攻修士課程修了．同年 NEC 入社，現在，NEC サービスプラットフォーム研究所ユビキタス基盤テクノロジーグループ主任研究員．携帯端末とそのユーザインタフェース，画像処理の研究を経て，センサネットワーク，人と環境のセンシング，およびそれらを活用したユビキタスサービスの研究に従事．