Vol.2013-CSEC-62 No.17
Vol.2013-SPT-6 No.17
2013/7/18

大規模ネットワークにおいてのセンサネットワーク向け鍵共有方式の比較評価

金子良[†1]　　岩村惠市[†2]

センサネットワークを流れる情報にはプライバシー情報が含まれる場合が多い．そのため，データの暗号化が必要であり，そのための鍵共有方法が重要である．SCIS2010 では大網らによって効率的な鍵共有法が提案されている．しかし，この方式はネットワークに参加するノード数が多いほど，多くの鍵を持たなければならない．
一方，ノードの論理構成を階層的に配置することにより，ノード ID を共有するだけで鍵共有が可能な階層型鍵共有方式が提案されている．本稿では，この二つの方式を大規模ネットワークを前提にしたシミュレーションを行い，その有用性を比較した．ただし，両方式の前提を同じにするために，鍵共有後ノードの要素鍵はハッシュ関数によって更新されるとした．

Comparative evaluation of large scale sensor network for key management

RYO KANEKO[†1]　KEIICHI IWAMURA[†2]

Privacy information, in many cases, is included in the information flowing through sensor networks. Therefore, effective data encryption is needed to ensure security, and an efficient key management scheme is required. At SCIS2010, Ooami presented an efficient key management scheme for sensor networks. However, in his method, a larger number of participating nodes required a larger number of keys, and the method to prevent key analysis was to renew the element key. On the other hand, some authors have presented a hierarchical key management scheme that is based on sharing of node IDs. In this study, we investigate a large-scale network-based simulation that is conducted using these two methods and compare their performance.

1. はじめに

センサネットワークとは，複数のセンサノードによって構成されるネットワークである．センサノードはセンシング機能を持ち，観測したデータを無線通信で送受信できる小型な端末である．また，これらのノードは基地局を介すことなく通信を行うことができる．このセンサノードを大量に散布することにより，広範囲な環境情報を収集することができるため，環境測定や 農業など様々な場面での活躍が期待されている．これらのセンサネットワークではセンサノードにより観測されたデータの中にプライバシー情報が含まれる場合があり，無線通信を使用し誰でも受信可能であるためデータの暗号化が必要である．しかし，これらのセンサノードは物理的に安全ではない場所に設置されることが多く，ノードの盗難によって攻撃者に暗号通信に必要な鍵情報を解析される可能性がある．また，センサノードは限られた電源容量，演算能力しか持たない．そのため，少ない計算量で暗号鍵を安全に共有でき，また，漏洩した情報から他ノード間の暗号通信の安全性が損なわれないような鍵管理方式が必要となる．

†1 東京理科大学工学研究科電気工学専攻，〒125-8585 東京都葛飾区新宿 6-3-1, Tokyo University of Science, 6-3-1 Shinjuku, Katsushikaku, Tokyo, 125-8585, Japan,kaneko_r@sec.ee.kagu.tus.ac.jp

†2 東京理科大学工学部第一部電気工学科，〒125-8585 東京都葛飾区新宿 6-3-1, Tokyo University of Science, 6-3-1 Shinjuku, Katsushikaku, Tokyo, 125-8585, Japan, iwamura@ee.kagu.tus.ac.jp

そこで，センサネットワーク向けの鍵管理方式として複数のトポロジに適用可能な鍵管理方式(以下，大網方式)[1]が提案されている．従来方式の多くは新規ノードを追加しない静的なネットワークやある特定のトポロジを対象としており，汎用性が持たない．これに対して，大網方式は接続トポロジの変化や新規ノードの追加等ネットワークの拡張に対応している．また大網方式は，高い可用性や耐盗難性を持たせることが可能である[1]．可用性とはトポロジや接続ノードを予見することなく鍵共有が成功する性質である．また，耐盗難性とはあるノードが盗まれ鍵を解析されたとしても他の暗号通信に影響を与えない性質であり，ネットワークに存在する鍵の漏洩率である鍵危殆化確率で評価される.大網方式は全ノードに共通のグローバル鍵を有するため高い可用性が実現できる．しかし、この鍵だけで鍵共有を行うと耐盗難性が弱くなるため、ランダムに選択されたランダム鍵で鍵共有を行えるようにしなければならない．そのためには、1 台のノードが所有する鍵の数を多くしなければならないという問題点をもつ．メモリ容量が少ないセンサノードでは，所持する鍵の数は少なく抑えることが望ましい．

そこで，1 台のノードが所有する鍵の数を少なく抑える方式として，階層型鍵共有方式[2,3]が提案されている．階層型鍵共有方式では，対称マトリックスと呼ばれる行列を階層的に配置し，各ノードに鍵配列を要素鍵として格納することで各ノードの所持する鍵の個数を大きく削減してい

Vol.2013-CSEC-62 No.17
Vol.2013-SPT-6 No.17
2013/7/18

る．また，階層型鍵共有方式は大網方式と違い，全てのノードが確定的に鍵共有を行うことができる．

ここで，全てのノードが鍵共有を完了したあとに全要素鍵が更新され、ノードが盗難されたとしても，そこからは暗号通信に影響を与えないとする．多くの鍵管理方式では解析されるノードの数が多いほど，すなわち盗難されるノード数が多いほど鍵危殆化確率が大きくなる．よって，鍵共有を完了する時間が早く終われば盗難され，解析されるノードの数も減ることになる．そのため，耐盗難性を評価する際に各ノードが鍵共有を完了する時間は重要な要素であると考えられるが，研究用に大量のセンサノードを用いる大規模ネットワークの構築することは困難であるため，今までその時間が評価されることはなかった．

本稿では，「QualNet」というネットワークシミュレータを用いて大網方式と階層型鍵共有方式において各ノードが鍵共有を完了する時間の面を踏まえて耐盗難性の評価を行った．そして，その結果から大網方式と階層型鍵共有方式のどちらが実用的であるかの検討を行った．

以下，第 2 章ではセンサネットワークの概要について，第 3 章では大網方式と階層型鍵共有方式について説明する．そして，第 4 章では評価をするにあたって使用したネットワークシミュレータ「QualNet」について説明し，第 5 章で実験方法，実験結果について述べ，第 6 章でむすびとする．

2. センサネットワーク

センサネットワークとは，複数のセンサノードによって構成されるネットワークである．センサノードは非常に安価なものであり，電池容量やメモリ，CPU の能力など限られた資源しか持たない．また，センサノードはセンシング機能を持ち，観測したデータを無線通信で送受信できる小型端末であり，基地局を介すことなく通信を行うことができる．このセンサノードを大量に散布することにより，広範囲な環境情報を収集することができる．実際に，センサネットワークは農業の分野では，農園にセンサノードを設置することで気象データや作物の生育情報を収集，分析することで，適正な作物の収穫時期の見極めや，害虫，病害対策を適切なタイミングで実施できるようになるなど，実用化されつつある．今後，防災・災害予測，防犯・セキュリティ，医療・介護，交通などさまざまな分野で利用されることが期待されている．

本章では，センサネットワークを構成するノードの特徴と接続トポロジについて述べる．

2.1 センサネットワークの構成

一般に，センサネットワークなどで用いられるセンサノードは，ベースステーション，ルータ，エンドデバイスの 3 種類で構成される．ベースステーションはネットワーク全体の管理機能を持つノードであり，ルータはノードからノードへデータを中継するルーティング機能を持つ．エンドデバイスはデータのセンシングを行い，その結果を送信するだけの末端ノードとして働く．本稿では，ルータとエンドデバイスを総称して子ノードと呼ぶ．

2.2 接続トポロジ

センサネットワークでは，上記のようなノードを組み合わせ，使用用途に応じて最適な接続トポロジを構成する．図 1 は各トポロジの構成例である．しかし，ノード間の通信が障害物などによって遮断された場合などは，迂回するために接続トポロジを切り替える状況が想定される．例えば，遮断されたスター型の一部にメッシュ型を組み合わせることで，ベースステーションと直接通信できなくなったノードでも，隣接ノードを介してデータをベースステーションに送信することが可能となる．このように，複数の接続トポロジに柔軟に対応できる鍵管理方式は，種々の用途に用いることができるため有用性が高い．

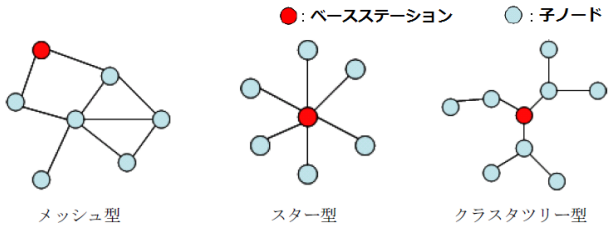

図 1　センサネットワークの接続トポロジ例

Figure1　Examples of connection topology of the sensor network.

2.3 ネットワーク拡張

本稿では，ノードは初期配置された場所から移動しないとする．このような，一度センサノードを配置し鍵共有を行った後に新規ノードの追加を考えないネットワークを静的ネットワークと呼ぶ．一方，新規ノードを追加して既存のネットワークを拡張するネットワークを動的ネットワークと呼ぶ．静的ネットワークを構築後に．新たなエリアのデータを得るため新規ノードを追加することが考えられることから，静的ネットワークと動的ネットワークのどちらにも対応できる鍵管理方式は重要となる．

3. 既存研究

センサネットワークを向け鍵管理方式は一般的に表 1 の要件を満たすことが望ましい．

センサネットワーク向け鍵管理方式としては，鍵事前格納方式が研究されている．鍵事前格納方式とは工場出荷時などに予め要素鍵と呼ばれる鍵を格納し，その鍵を用いることで実際に暗号化通信に必要なリンク鍵の生成を行う方式である．鍵事前格納方式はいくつも提案されているが，主に確率的鍵事前格納方式と確定的鍵事前格納方式の 2 種類に分類できる．

Vol.2013-CSEC-62 No.17
Vol.2013-SPT-6 No.17
2013/7/18

表 1　センサネットワーク向け鍵管理方式の要件
Table1 Requirements of the sensor network for key management.

・計算量	センサノードは限られた演算能力しか持たず，公開鍵暗号など複雑な計算を行うことが難しい.
・メモリ	センサノードは限られたメモリ容量しか持たないため，事前に格納する鍵の数を少なくすることが望ましい.
・可用性	隣接ノードと暗号化通信に必要なリンク鍵の生成が行える性質.
・耐盗難性	攻撃者によってノードが盗難され解析された際に，その情報から他の暗号化通信の情報が漏えいしない性質.

確率的鍵事前格納方式[1,4,5]とは，鍵プールと呼ばれる要素鍵の集合を用意し，その中からランダムにノードに鍵を割り当てていく．リンク鍵の生成には，各ノードが持つ鍵の情報を交換することで， 共通な鍵を認識し，その鍵をリンク鍵の生成に利用する方式である．しかし， 要素鍵をランダムに割り当てているため， 確実に鍵共有を行うことができない．そこで，可用性を高める方式が提案されているが，鍵共有は確率的であるため，大規模なネットワークでは鍵共有を行うことができないノードが存在してしまうことになる．

確率的鍵事前格納方式に対して確定的鍵事前格納方式[2,3,6,7,8,9,10]とは，要素鍵によって各ノードが確実に暗号化に使用するリンク鍵を生成できる方式である．確定的鍵事前格納方式は確率的鍵事前格納方式に比べ，各ノードが保有しなければならない要素鍵の数を少なくできる．しかし，各ノードは隣接ノードと確実にリンク鍵を生成するために規則的に要素鍵を配置する場合が多く，攻撃者によってノードが盗難され，解析された時に影響を受けるリンクの数が多くなってしまうという欠点を持つ．

以下に確率的鍵事前格納方式である複数のトポロジに適応可能な鍵管理方式と確定的鍵格納方式の階層型鍵共有方式について説明する．

3.1 複数のトポロジに適用可能な鍵管理方式(大網方式)[1]

3.1.1 事前準備

ノードは以下の 6 つの要素を持って配置されてから，3.1.2 節から 3.1.6 節で説明するそれぞれのトポロジに対応した鍵共有を行う．

・固有鍵：k_u
・グローバル鍵：k_G
・ランダム鍵（複数個）k_r
・チケット：T
・固有鍵リスト（ベースステーションのみ）

固有鍵とはそれぞれのノードが独自に持つ鍵であり，重複しないとする．グローバル鍵とはすべてのノードが共通して持つ鍵である．ランダム鍵は図 2 に示すように，予め用意された複数個の鍵集合である鍵プールから 1 つずつランダムに選択され格納される鍵である．また，ランダム鍵にはそれぞれ鍵 ID が割り振られている．そのため，ノード同士で鍵 ID を交換することでお互いが所有するランダム鍵を認識することができる．

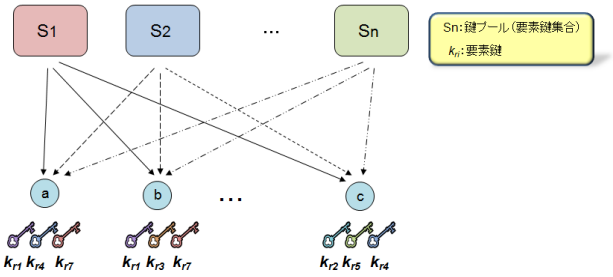

図 2　ランダム鍵の格納
Figure2　How to store the random key.

チケットは，以下の式のように表される．

$$T = k_{uc}(k_u \| t_D \| K \| r) \qquad (1)$$

チケットは，各ノードの固有鍵 k_u，チケットの失効期限 D_t, 保有するすべてのランダム鍵を連接し，そのハッシュ値をとって生成したリンク鍵 K，乱数 r を連接し，ベースステーションの固有鍵 k_{uc} で暗号化したものであり，同一のチケットが生成されることはない．失効期限 D_t は *YYYY* 年 *MM* 月 *DD* 日 *hh* 時 *mm* 分 *ss* 秒のように定義されている．チケットはベースステーションの固有鍵 k_{uc} で暗号化されているので，復号できるのはベースステーションのみであり，チケットの失効期限はベースステーションのタイマーによって判断される．固有鍵リストは新規追加を含むすべてのノードの固有鍵が記されているものであり，ベースステーションのみが所有する．また，要素鍵を更新する時間が定められており，一定時間ごとに要素鍵の更新を行う．攻撃者が鍵共有を完了後にノードを盗難，解析して更新後の要素鍵を得たとしても，暗号通信に使用するリンク鍵に関する情報は一切得られない．つまり，鍵の更新を行うことによって耐盗難性を高めることができる．

3.1.2 静的メッシュ型トポロジにおける鍵共有

それぞれのノードはグローバル鍵とランダム鍵を用いて，近接するノードと 1 対 1 で鍵共有を行う．すべての鍵にはそれぞれに対応する鍵 ID が割り振られており，それを交換することでお互いが持つ鍵を知ることができる．まず，ノードは互いの所有するランダム鍵の鍵 ID を交換し，共通して持つ鍵を認識する．そして，その共通して持つ鍵を連接し，一方向性ハッシュ関数に入力してリンク鍵を生成する（(2)式）．すべてのノードにはグローバル鍵は格納されているため，必ず鍵共有を行うことができる．

$$K = h(k_{r1} \| \cdots \| k_{ri} \| k_G) \qquad (2)$$

K：リンク鍵，h：一方向性ハッシュ関数
k_r：ランダム鍵，k_G：グローバル鍵

3.1.3 静的・動的スター型トポロジにおける鍵共有

子ノードからベースステーションにチケットを送信する．ベースステーションは受信したチケットを復号し，子ノードの固有鍵を固有鍵リストと照合し，チケットの失効期限を確認する．チケットが正当と認められれば子ノードの固有鍵をリンク鍵とし保持する．不当であった場合は接続を切断する．

3.1.4 動的メッシュ型トポロジにおける鍵共有

追加される新規ノードがベースステーションではなく子ノードと接続する可能性が考えられる．その場合は，新規ノードからチケットを受け取った子ノードはベースステーションにチケットを送信する．チケットを受信したらベースステーションは 3.1.3 節と同様に認証を行う．正当であった場合は，新規ノードの生成可能なリンク鍵を子ノードの固有鍵で暗号化したものを子ノードに送信する．新規ノードと子ノードはこのリンク鍵を用いて鍵共有を行う．

3.1.5 静的クラスタツリー型トポロジにおける鍵共有

ベースステーションと直接接続しているノードは 3.1.3 節と同様で，ベースステーション以外と接続しているノードは 3.1.2 節と同様に鍵共有を行う．

3.1.6 動的クラスタツリー型トポロジにおける鍵共有

新規ノードがベースステーションと直接接続する場合は 3.1.3 節と同様で，ベースステーション以外と接続する場合は 3.1.4 節と同様である．

3.2 階層型鍵共有方式[2,3]

3.2.1 対称マトリックスを用いた鍵共有

階層型鍵共有方式に必要な対称マトリックスを用いた共通鍵の格納方法について簡単に説明する．

・事前準備

①要素(i, j)と要素(j, i)が等しい配列(対称マトリックス)を準備する.(図 3①)

②ノードに自身のノード ID にあたる列を格納.(図 3②)

・共通鍵の認識

③ノード ID を交換し，格納された配列を参照することで共通鍵を得る.(図 3③)

3.2.2 事前準備

ノードは以下の 4 つの要素を持って配置されてから，3.1.2 節から 3.1.6 節で説明するそれぞれのトポロジに対応した鍵共有を行う．

・固有鍵：k_u
・鍵配列：G_{hi} ($(h \times i)$ 個)
・チケット：T
・固有鍵リスト（ベースステーションのみ）

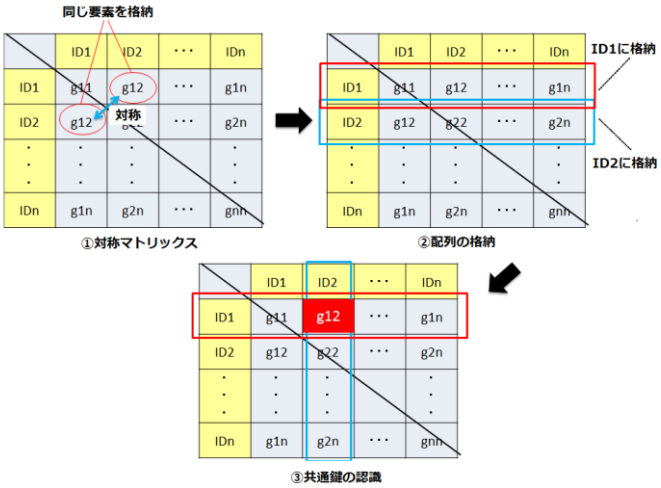

図 3　対称マトリックスを用いた鍵共有
Figure3 Key Sharing Based on the symmetric matrix.

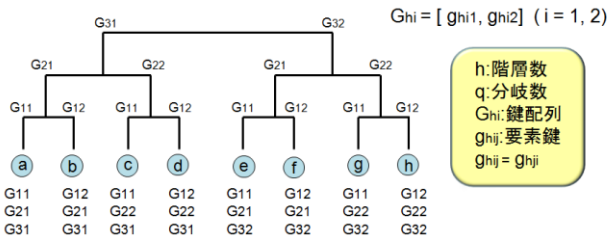

図 4　階層型鍵共有方式における要素鍵の格納
Figure4　Storage of key elements in hierarchical key management scheme.

階層型鍵共有方式では，大網方式と同様，固有鍵，チケット，固有鍵リストを持つ必要がある．大網方式におけるランダム鍵，グローバル鍵の格納の代わりに以下の方法を用いて要素鍵として鍵配列を格納する．各階層には階層数 h，分木数 i に対応した鍵配列 G_{h1}, G_{h2} ,…, G_{hi} が準備される．階層数および分岐数は全ノード数に応じて適宜設定する．また，各ノードは階層構造の端点に割り当てられ，自身が対応している分木の鍵配列が格納される．そのため，各ノードは階層数分の鍵配列を所持し，所持する鍵の個数は(階層数 h)×(分木数 i)個となる．また，鍵配列を構成する要素鍵は上記で説明した対称マトリックスを利用しており，$g_{hij} = g_{hji}$ とする．鍵共有はノード ID のみを交換し，鍵配列の中から共通して所有する鍵を認識する．図 4 では階層数 h=3，分岐数 i=2 である．この場合各ノードが所持する鍵配列は 3 個であり，鍵の数は 6 個である．

また，大網方式と同様に一定時間ごとに要素鍵の更新を行うことで，耐盗難性を向上させている．

3.2.3 静的メッシュ型トポロジにおける鍵共有

鍵共有をするノード同士でノード ID を交換する．ノードは受信したノード ID を用いて鍵配列の中から共通して所有する鍵を認識する．リンク鍵の生成では大網方式と同様に，共通して持つ鍵を連接し一方向性ハッシュ関数を用いてリンク鍵を生成する（(2)’ 式）．

$$K = h(k_{g1} \| \cdots \| k_{gi}) \qquad (2)'$$

K：リンク鍵，h：一方向性ハッシュ関数
k_g：ノードが持つ共通鍵

3.2.4 その他のトポロジにおける鍵共有

その他のトポロジにおける鍵共有は大網方式と同様である．ただし，静的ネットワークにおけるノードがベースステーション以外と接続している場合の鍵共有は 3.2.3 節と同様に行う．

3.3 評価

3.3.1 耐盗難性

耐盗難性の評価として，攻撃者が盗難したノードから漏洩した鍵情報を基に他のノード間の暗号化通信のリンク鍵を知る確率について考察する．攻撃者が n'_1，n'_2，…，n'_c の c 台のノードを盗難し，それらに格納された要素鍵をすべて知ったとする．ここで，$K(n_i)$はn_iの持つ要素鍵をする．盗難された c 台のノードに $K(n_1) \cap K(n_2)$が含まれていた場合，攻撃者は n_1, n_2 間のリンク鍵を知ることができる．つまり，攻撃者がリンク鍵を知る確率は，

$$K(n_1) \cap K(n_2) \subset \bigcup_{i=0}^{c} K(n'_i) \qquad (3)$$

となる．これを鍵危殆化確率と定義する．
大網方式の鍵危殆化確率 e_1 は以下の式で与えられる．

$$e_1 = \frac{1}{p}\left[\left\{1-\frac{1}{t}\left(1-\frac{1}{t}\right)^{c}\right\}^{m} - \left(1-\frac{1}{t}\right)^{m}\right] \qquad (4)$$

ここで，p はリンク鍵共有確率，t は鍵プール 1 つあたりの鍵数，m はノード 1 台あたりに格納される鍵数である．

また，階層型鍵共有方式における鍵危殆化確率 e_2 は以下の式で与えられる．

$$e_2 = \sum t_s p_c^{\,s} \qquad (5)$$

ここで，t_s は $K(n_1) \cap K(n_2)$が共通鍵をそれぞれの個数持つ確率であり，$p_c^{\,s}$ は攻撃者が $K(n_1) \cap K(n_2)$間のリンク鍵を知る確率である．それぞれ以下の式で与えられる．

$$t_s = \frac{{}_hC_a \times n^h \times (n-1)^{(h-a)}}{2} \times \frac{1}{{}_NC_2} \qquad (6)$$

$$p_c^{\,s} = \{1-(1-2q)^c\}^s \qquad (7)$$

以下に，大網方式と階層型鍵共有方式における盗難ノード数に対する鍵危殆化確率の比較を示す．なお，評価するにあたって，大網方式と階層型鍵共有方式の条件を同じにするために全ノード数 N を 10000 台とし，各ノードが持つ要素鍵の数を 40 個とする．つまり，大網方式では鍵プールの数を 40 個し，階層型鍵共有方式では，分岐数 10，階層数 4 とした．

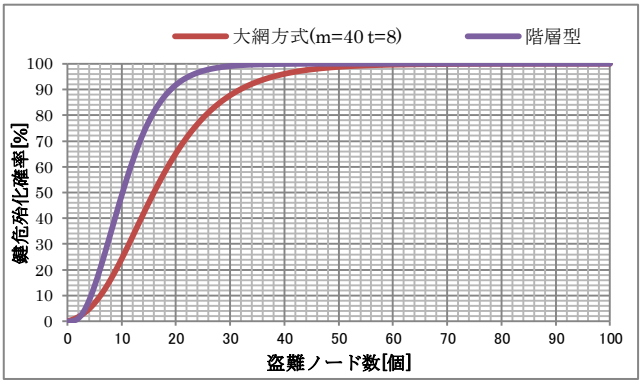

図 5　耐盗難性の比較

Figure5　Evaluation of resistance to theft.

各ノードが同じ数の鍵を保有している場合，耐盗難性は大網方式の方が有利であることがわかる．

ここで，耐盗難性は，盗難ノード数が増えるに従って大きくなってしまう．大網方式では，初期鍵失効時間により各ノード自身が持つランダム鍵を一定時間後にすべて削除する．つまり，鍵共有を完了するとそれ以上ノードが盗難されても，攻撃者にリンク鍵に関する情報は漏えいしない．初期鍵失効時間は，階層型鍵共有方式でも適応できる．そのため，多くのノードが盗難されないよう早く鍵共有を完了することが重要である．この二つの方式において共通鍵を認識するために交換しなければいけない情報は，大網方式では，自身のノード ID とランダム鍵の鍵 ID(格納された個数分)であるのに対し，階層型鍵共有方式では自身のノード ID のみである．鍵情報の送信には階層型鍵共有方式の方が時間はかからないと考えられるため，鍵共有を完了するまでの時間を踏まえた耐盗難性の評価を行うことが必要である．

4. QualNet

QualNet[11,12] は，アメリカの Scalable Network Technologies 社が開発している商用ネットワークシミュレータである．日本では，構造計画研究所が代理店を務めている．QualNet の最大の特徴は，シミュレーションエンジンの高速性とスケーラビリティである．マルチコア，分散処理に対応しており，数千のノードの大規模なネットワークをシミュレーションすることができる．また，標準規格を細部まで忠実に実装したプロトコルモデル，ワイヤレスモデル(パスロス，シャドウイング，フェージング)やモビリティモデルや地形情報など，シミュレーションモデリングに必要な要素が予め用意されており，さまざまな環境条件や運用条件に対するネットワーク性能の正確な予測を得ることができる．さらに，全てのモデルライブラリは，C++のソースコードで提供され，公開されている．プロトコルの改良やオリジナルの作成，出力処理の追加などを制限な

く行うことができ自由度の高いシミュレーションを行うことができる．

本研究では，実際の運用を想定し大規模なネットワークを構築した時のシミュレーションを行う．また，センサネットワーク向けのモデルライブラリも充実しているため，QualNet を使用し，実験を行った．

5. 実験

本実験では，ネットワークシミュレータ「QualNet」を用いて，大網方式と階層型鍵共有方式において大規模ネットワークでの鍵共有が完了する時間を測定する．

5.1 前提条件

各ノードはそれぞれ配置され，同時に鍵共有を開始することを想定する．また，各ノードはメッシュ型の接続トポロジを形成しているとする．さらに，リンク鍵生成に一方向性ハッシュ関数の計算をするのみなので時間はかからないとした．

5.2 実験の流れ

各ノードが鍵共有を完了するまでの流れを示す．

1. 各ノードは，隣接ノードに対して鍵共有に必要なデータをブロードキャスト通信で送信する
2. 鍵共有に必要なデータを受信したノードは，リンク鍵を生成する
3. 鍵共有完了

しかし，本実験に使用する QualNet では，アプリケーションプロトコルとしてのブロードキャスト通信は想定されていないため実装されていない．そこで，マルチキャスト通信を用いてを疑似的にブロードキャスト通信を行うことで，想定した鍵共有が行えるようにした．マルチキャスト通信とは，マルチキャストグループを指定し，そのマルチキャストグループに所属しているノード全てにデータを送信するものである．全てのノードを同じマルチキャストグループに所属させることで，ブロードキャスト通信と同じように隣接ノードすべてに対して同時に通信を行うことができる．また，マルチキャスト通信の場合には，ブロードキャスト通信と違い，どのノードが同じマルチキャストグループに所属しているかあらかじめ知る必要がある．そのため，本シミュレーションでは，マルチキャストルーティングプロトコルにより，あらかじめマルチキャストグループを把握した状態から時間の測定を行う．

シミュレータ上での鍵共有が完了するまでの流れを示す．

(事前準備)
1. マルチキャストルーティングプロトコルにより，マルチキャストグループを把握
(測定開始)
2. 各ノードは，隣接ノードに対して鍵共有に必要なデータをマルチキャスト通信で送信する
3. 鍵共有に必要なデータを受信したノードは，リンク鍵を生成する
4. 鍵共有完了

１つのノードは，隣接ノードすべてから鍵情報を送られる．そのため，本実験では隣接ノードから最後に鍵情報を受け取った時間を鍵共有が完了した時間として測定した．また，それぞれのノードの受信電力，送信電力の測定を行った．

5.3 測定条件

シミュレーションでは，50 個，100 個，1000 個のノードを正方形領域にランダムに配置した．ノードの通信距離は 30m とし，シミュレーション領域はノードの密度が同じになるように設定した．また，大網方式で鍵共有をするために送信しなければならないランダム鍵の鍵 ID は 32bit とし，階層型鍵共有方式で送信しなければならない各のノードのノード ID は 32bit とした．送信データサイズは 32Byte，100Byte，10000Byte の 3 パターンについてシミュレーションを行った．つまり，各ノードが保有する大網方式におけるランダム鍵がそれぞれ 8 個, 25 個, 250 個の場合である．データの送信プロトコルは MCBR を使用し，通信規格は IEEE 802.15.4（Zigbee）を使用した．ここで，センサネットワークでは一度に送信できるパケットのサイズは 100Byte ほどであるため 1000Byte のデータは一度に送信することはできない．そこで，100Byte のデータを 10 個に分けて 1mS 間隔で送信を行う．

シミュレーションの測定条件をまとめたものを以下に示す．

表 2　シミュレーションの実行環境
Table 2　Execution of the simulation environment.

シミュレーションソフト	OS	CPU	メモリ
QualNet 5.2	windows7 professional	Intel corei7 970	12GByte

表 3　シミュレーション条件
Table 3　The simulation conditions.

ノード数(個)	50，100，1000
シミュレーション領域	正方形領域
ノード配置	ランダム
鍵 ID サイズ(bit)	32
送信データサイズ(Byte)	32，100，1000
要素鍵の個数(個)	8，25，250
通信規格	IEEE 802.15.4
送信プロトコル	MCBR

表 4　シミュレーション領域の詳細
Table 4　Details of the simulation region.

ノード数	正方形領域
50 個	135m×135m
100 個	195m×195m
1000 個	600m×600m

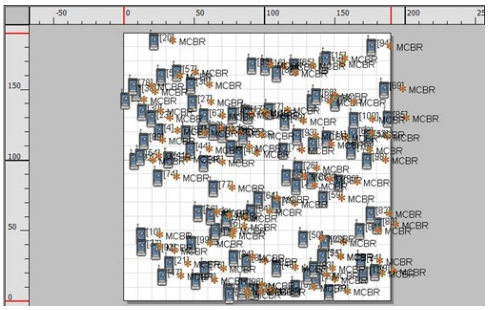

図 6　シミュレーションでのノードの配置(例)
Figure6 Example of the arrangement of nodes in the simulation.

5.4 実験結果

ノードが鍵共有を完了するまでの時間の実験結果を表 5 に示す．なお，ノードに配置は 10 パターンで測定を行い，平均値をとったものを結果として表示する．

結果から，送信データサイズが一定の時，鍵共有に完了する時間はノード数が増えてもほとんど差異はないことがわかる．また，ノード数が一定の時，データサイズを大きくするにつれて鍵共有が完了する時間は増えていくことはわかる．配置するノード数が 1000 個で，送信データサイズが 1000Byte の場合でも 3 秒ほどで鍵共有を完了するため，わずかな時間で鍵共有が完了するといえる．しかし，送信データサイズが 32Byte の時に比べ 1000Byte の鍵共有が完了する時間は約 10 倍の時間がかかっている．

次に，表 6，7 にノードの送信電力，受信電力の実験結果を示す．結果から，ノード数が多くなる，または，送信データサイズが大きくなると消費電力が大きくなることがわかる．送信電力に対して，受信電力が多くなっているのは，各ノードが鍵共有を行うために送信より受信を多く行う必要があるためである．また，鍵共有を行うのに必要な消費電力である，送信電力と受信電力の合計は最大の場合でも 19 μ Wh ほどである．ここで，センサノードは，乾電池二本ほどで駆動することが想定されているが，乾電池一本の電力量は 1.5Wh ほどである．つまり，一度の鍵情報の送信で鍵共有ができるとすると，鍵情報の送受信に必要な電力は電池に対して非常に小さいといえる．

表 5　鍵共有が完了する時間[s]
Table 5　The time to complete the key sharing．[s]

	データサイズ[Byte]（要素鍵の数[個]）			
ノード数[個]		32(8)	100(25)	1000(250)
	50	0.1890	0.3158	1.5993
	100	0.1933	0.3089	2.4593
	1000	0.2372	0.3585	2.4617

表 6　送信電力の比較[μ Wh]
Table 6　Comparison of the transmission power．[μWh]

	データサイズ[Byte]（要素鍵の数[個]）			
ノード数[個]		32(8)	100(25)	1000(250)
	50	0.439	0.492	1.391
	100	0.438	0.489	1.805
	1000	0.437	0.877	2.997

表 7　受信電力の比較[μ Wh]
Table 7　Comparison of the received power．[μWh]

	データサイズ[Byte]（要素鍵の数[個]）			
ノード数[個]		32(8)	100(25)	1000(250)
	50	2.014	2.102	5.919
	100	2.087	2.332	8.810
	1000	2.217	4.658	15.21

5.5 評価

大網方式と階層型鍵共有方式においての耐盗難性について鍵共有を完了する時間を踏まえた評価を行う．階層型鍵共有方式が隣接ノードに送信しなければならない鍵情報はノード ID のみなので，送信データサイズは 32Byte 以内に収まる．表 5 より，送信データサイズが 32Byte の時に比べ 1000Byte の鍵共有が完了する時間は約 10 倍の時間がかかっていることが分かった．すなわち，大規模ネットワークを構成することを考えた場合，階層型鍵共有方式に対して大網方式が鍵共有を完了する時間は約 10 倍かかってしまうことが分かる．ここで，階層型鍵共有方式において，攻撃者が鍵共有を完了す前にノードを盗難できるとすると，大網方式はその 10 倍の数のノードが盗難されることになる．つまり．盗難されるノードの数に大きく差が出るため，階層型鍵共有方式の方が耐盗難性は有利であると考えられる．また，階層型鍵共有方式において，攻撃者が鍵共有を完了する前にノードを盗難できないとすると，大網方式と階層型鍵共有方式で盗難されるノードの数にあまり差がないと考えられるので，大網方式の方が耐盗難性は有利であると考えられる．

6. おわりに

本稿では，従来方式である大網方式と階層型鍵共有方式においての耐盗難性を鍵共有が完了する時間を踏まえた評価を行った．特に，「QualNet」というネットワークシミュレータを使って従来は行われていなかったセンサネットワークのセキュリティに関する大規模ネットワークのシミュレーションを行った．鍵共有を完了する時間は，ノード数，送信する鍵情報が増えるにつれて大きくなる．よって，耐盗難性は，攻撃者が階層型鍵共有方式が鍵共有を完了する前にノードを盗難できるとすると，階層型鍵共有方式の方が耐盗難性は有利であることがわかった．ただし，攻撃者

によって鍵共有を完了する前にノードを盗難できないとすると，大網方式の方が耐盗難性は有利である．

本稿では，特定の状況下のみのシミュレーションしか行っていない．そのため，今後の課題としては様々な状況を想定したシミュレーションを行う必要があると考えられる．

参考文献

1) 大網優太, 柿崎淑郎, 岩村惠市, “センサネットワークにおける複数のトポロジに適用可能な鍵管理方式の提案”, 2010 年暗号と情報セキュリティシンポジウム SCIS2010), 3C2-5，January 2010.
2) 岩村 惠市,山本 貴久, 特許広報 通信方式及びそのシステム,特許第 3548215 号
3) 齊藤 壮馬，岩村 惠市, “低消費電力と高安全性を両立する新しい LEACH プロトコル”，第 61 回コンピュータセキュリティ研究会(CSEC), May.2013
4) 松本 律子, 毛利 寿志, 楫 勇一, “複数の小規模鍵プールからの鍵選択に基づくセンサノード鍵格納方式,” SCIS2006, 3D4-4, 2006.
5) H. Yukimaru, Y. Kakizaki, and K. Iwamura. Key management scheme applicable to various topologies of sensor networks. In Proc. of Sixth International Conference on Availability, Reliability and Security (ARES-2011), pp. 448–453. IEEE CS, August 2011.
6) 伊豆 哲也, 武仲 正彦, 鳥居 直哉, “センサネットワークにおける効率的な鍵共有方式”，2010 年 コンピュータセキュリティシンポジウム(CSS2010), 1D1-1, October 2010.
7) 酒見 由美, 伊豆 哲也, “センサネットワークにおける効率的な事前共有鍵の配布方法,” SCIS2013, 2F1-3, 2013.
8) 大網優太，齊藤誠，岩村惠市, “センサネットワークにおける鍵事前格納方式に関する一提案”，第 39 回コンピュータセキュリティ研究会，pp.37-42．Dec.2007.
9) 飯田 達郎, 宮地 充子, 面 和成, “マルチフェーズワイヤレスセンサネットワークにおける効率的かつセキュアな鍵共有方式”, 2010 年 コンピュータセキュリティシンポジウム(CSS2010), 1D2-3, October 2010.
10) 飯田 達郎, 面 和成, 宮地 充子, “ワイヤレスセンサネットワークにおける自己治癒機能を有する鍵共有方式の検討”，第 52 回コンピュータセキュリティ研究会(CSEC),5-B ,March.2011
11) QualNet, (構造計画研究所)
http://network.kke.co.jp/products/qualnet/
12) 高木由美, 太田能, ”QualNet によるネットワークプロトコル性能評価-GUI 環境とシミュレータアーキテクチャ-”IEICE, 2009