Vol.2013-CSEC-61 No.14
Vol.2013-IOT-21 No.14
2013/5/10

センサネットワークの鍵共有に関するシミュレーション評価

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，この手法は，ネットワークに参加するノード数が多くになるほど，鍵共有の際に多くの要素鍵を隣接ノードに知らせらければならない．本論文では，大網方式における要素鍵の数による鍵共有時間への影響をシミュレーションにより評価する．特に，QualNet というネットワークシミュレータを用いて，センサネットワークのセキュリティに関する大規模シミュレーションを行う．

Evaluation of sensor network simulation on shared key.

RYO KANEKO[†1]　KEIICHI IWAMURA[†2]

Often contain privacy information of the information flowing through the sensor network. Therefore, it is necessary to encrypt the data, it is important key sharing method therefor. Efficient key sharing scheme has been proposed by Ooami in SCIS2010. However, as the number of nodes that participate in the network will be more, this approach must kick from the news to the adjacent nodes at the time of the key elements of many key sharing. In this paper, we evaluate by simulation the impact of key sharing time with the number of key elements in the process of Ooami. In particular, using a network simulator called QualNet, carried out large-scale simulation of a sensor network security.

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，交通，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化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．

そこで,センサネットワーク向けの鍵管理方式として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，その鍵を用いて実際に暗号化通信に用いるリンク鍵の生成を行う方式である．しかし，従来の方式[1][2]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に適しており，汎用性がなかった．それに対し大網等が提案した複数のトポロジに適用可能な鍵管理方式(以下大網方式)[3][4]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．さらに，大網方式は，他の方式に比べ可用性や耐盗難性についても優れている．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化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．

大網方式では初期鍵失効時間を設定し，一定時間が過ぎたら各ノード自身が持っているランダム鍵をすべて消去する．そのため，初期鍵失効時間によって，全てのノードが鍵共有を完了したあとにノードが盗難されたとしても，そこからは暗号化通信に影響を与えない．つまり，ノードの数が多いほど，鍵危殆化確率が大きくなるので，鍵共有を完了する時間が早く終われば，盗難され，ノードが解析されたとしても安全性は低下しない．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，鍵共有を完了する時間は数式だけでは解析困難である．よって，実際の運用を想定し，シミュレーションを行う必要がある．しかし，一般的に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．そこで本論文では，QualNet[5][6]というネットワークシミュレータを用いて，大網方式にお

†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@sec.ee.kagu.tus.ac.jp

ⓒ 2013 Information Processing Society of Japan

ける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．

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 章では複数のトポロジに適用可能な鍵管理方式の概要について説明する．そして，第 4 章では大規模ネットワークでのシミュレーションを行うに当たって使用した QualNet について説明し，第 5 章で実験の方法，結果について述べ，第 6 章でまとめとする．

2. 接続トポロジおよびネットワーク拡張

一般に，Zigbee 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．

2.1 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．

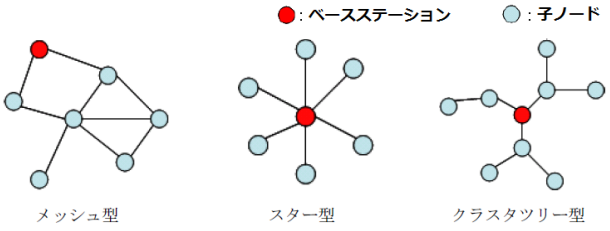


図 1　センサネットワークの接続トポロジ例

Figure1　Examples of connection topology of the sensor network.

2.2 ネットワーク拡張

本論文では，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. 複数のトポロジに適用可能な鍵管理方式[3]

3.1 前提条件

センサネットワークはベースステーションにより管理されているため，ベースステーションが盗難されることはネットワークが機能しなくなることに等しい．そのため，この方式ではベースステーションは耐タンパ性を持ち，安全に管理されているものとする．

3.2 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，3.3 節から 3.7 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）
- 初期鍵失効時間：t_s

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．

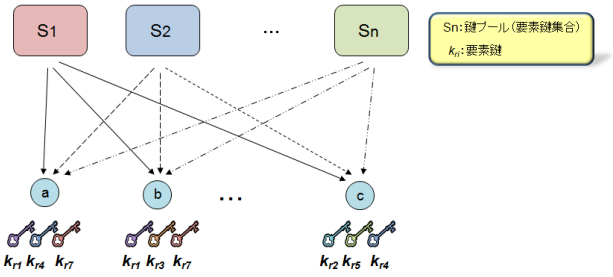


図 2　ランダム鍵の格納

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

ⓒ 2013 Information Processing Society of Japan

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，ノードには初期鍵失効時間が定められており，ノードは初期鍵失効時間以内に鍵共有を行わなければならず，鍵共有を行うか初期鍵失効時間になるとノードは自らが持つグローバル鍵とランダム鍵を削除する．これにより，初期鍵失効時間以降に鍵情報が漏洩することを防ぎ，耐盗難性を持たせている．

3.3 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

3.4 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．

3.5 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 3.4 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．

3.6 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 3.4 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 3.3 節と同様に鍵共有を行う．

3.7 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 3.4 節と同様で，ベースステーション以外と接続する場合は 3.5 節と同様である．

3.8 耐盗難性の評価

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 は以下の式で与えられる．

$$e = \frac{1}{p}(((1-\frac{1}{t}(1-\frac{1}{t})^c)^m - (1-\frac{1}{t})^m) \qquad (4)$$

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．

以下に，大網方式における盗難ノード数に対する鍵危殆化確率をグラフにしたものを以下に示す．なお，評価するにあたって，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．

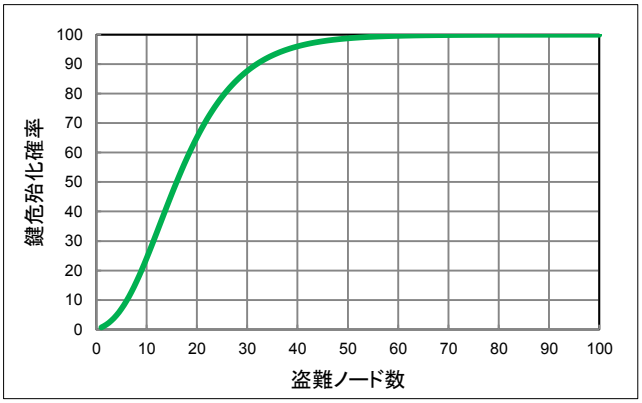


図 3　耐盗難性の評価

Figure3　Evaluation of resistance to theft.

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. 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．

4. QualNet

QualNet は，アメリカの Scalable Network Technologies 社[7]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

ⓒ 2013 Information Processing Society of Japan

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，同時に電源が入れられたことを想定する．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，リンク鍵生成には時間はかからないとする．

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，大網方式で送信しなければならないランダム鍵の鍵 ID は 32bit とし，送信データサイズが 32Byte，100Byte，10000Byte の３パターンにお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表 1，2，3 に示す．

表 1　シミュレーションの実行環境
Table 1　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 2　シミュレーション条件
Table 2　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

ⓒ 2013 Information Processing Society of Japan

表 3　シミュレーション領域の詳細

Table 3　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

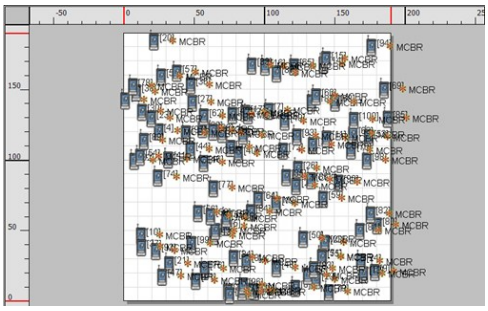


図 4　シミュレーションでのノードの配置(例)

Figure4　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測定結果を表 4 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．

測定結果から，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ことがわかる．

次に，表 5，6 にノードの送信電力，受信電力の測定結果を示す．測定結果から，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 3.0Wh 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 4　鍵共有が完了する時間[s]

Table 4　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 5　送信電力の比較[μ Wh]

Table 5　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 6　受信電力の比較[μ Wh]

Table 6　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

6. おわりに

本論文では，従来方式である大網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，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ことがわかった．また，鍵情報を隣接ノードに送受信するときの消費電力は電池に対して非常に小さくなることがわかった．

今後の課題としては，本論文では言及しなかったノードがリンク鍵の生成にかかる時間を踏まえた検討を行うことがあげられる．

参考文献

1) 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.
2) 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.
3) 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.
4) 雪丸 英俊，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実装”2010 年 コ

ⓒ 2013 Information Processing Society of Japan

ンピュータセキュリティシンポジウム(CSS2010)，1D2-1，October 2010.
5) QualNet(構造計画研究所)
http://www4.kke.co.jp/network/qualnet/index.html
6) 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
7) Scalable Network Technologies 社
http://web.scalable-networks.com/

ⓒ 2013 Information Processing Society of Japan