Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

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

飯田達朗[†1]　面和成[†1]　宮地充子[†1]

ワイヤレスセンサネットワーク（WSNs）を長期使用する際，WSNs への攻撃に対して Forward Secrecy（過去情報の秘匿）や Backward Secrecy（未来情報の秘匿），Self-Healing（センサの自己治癒）の特性が重要となる．我々は CSS2010 において，各センサが周りのセンサの協力を得て共有リンク鍵の更新を行うことにより，上記 3 つの特性を全て満たす鍵共有方式を検討した．しかし，共有リンク鍵の自己治癒機能やマルチフェーズ WSNs への適用に対する考察が不十分であった．本研究では，鍵の更新方法，効率的なマルチフェーズ WSNs への適用方法についてさらなる検討を行った．また，数式モデルによる理論値とシミュレーション実験によって安全性の確認を行った．

Proactive co-Operative Link Self-Healing for WSNs

Tatsuro Iida,[†1] Kazumasa Omote[†1]
and Atsuko Miyaji[†1]

When wireless sensor networks (WSNs) are used for a long term, the three requirements (Forward Secrecy, Backward Secrecy and Self-Healing) are important to recover secret information from attacks on WSNs. In CSS2010, we proposed a pairwise key establishment scheme that satisfies above three requirements by regularly updating a key using contributions from the sensors, where the sensor can self-heal using contributions from the non-compromised sensor. In this paper, we mainly discuss the security of our scheme by the analytical value and the experiment value.

†1 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

1. はじめに

ワイヤレスセンサネットワーク（WSNs）とは計算機能と無線機能を持つ多くのセンサから構成されるアドホックネットワークの一種である．WSNs においてセンサは物理的に保護されない場所に配置されることが多く，悪意のある攻撃者から盗難・盗聴といった攻撃を受ける危険性がある．そのため，暗号化などのセキュリティ技術を用いることで攻撃者へのデータ漏洩を防ぐ必要がある．しかし，一般的に WSNs で使用されるセンサは耐タンパ性を持たず，センサ自体を攻撃されるとセンサは秘密情報を漏洩（危殆化）してしまう．また，センサの性能はごく限られた電源容量と演算性能であるため，計算量が大きい公開鍵暗号技術等は利用しないことが多く，センサには生存期間（使用期限）が設けられる．

上記の制限のもと，WSNs の安全性を確保するため，共通鍵暗号技術が使用される．しかし，全センサに共通の鍵を持たせてしまうと，1 つのセンサが危殆化しただけで全ての通信やストレージが危殆化してしまうという問題がある．この問題に対して，RKP 方式[3] が Eschenauer 等によって提案された．RKP 方式では，センサ配置前にランダムな鍵の集合から各センサへ複数の鍵を割り当て格納する．センサ配置後，センサ間に共通する鍵が存在した時，その鍵を共有リンク鍵として用いることで暗号通信を行うリンクを構成する．そのため，一部の鍵が漏洩しても WSNs 全体の通信の安全性は維持できる．Chan 等は共有リンク鍵の構成に q 個以上の鍵を組み合わせることで RKP 方式の安全性を向上させた $q-$ 複合鍵方式[2] を提案した．さらに，Liu 等は $q-$ 複合鍵方式で用いられている鍵プールを 2 変数多項式プールに変更した方式[6] を提案した．しかしながら，これらの鍵共有方式を WSNs で用いる際，攻撃を受けたセンサの安全性は元に戻らないため，時間とともに危殆化した鍵が増え，WSNs の安全性が低下してしまう．そのため，鍵更新やサーバの補助を利用して安全性を自己治癒する方式が提案された．Castelluccia 等が提案した RoK 方式[1] では，ハッシュ関数を用いて鍵を定期的に更新することで攻撃者が盗聴できるリンクの割合を低く抑え，高い安全性を維持することができる．また，RoK 方式は，ネットワーク内のセンサを定期的に新規センサと交換する WSNs（マルチフェーズ WSNs[4),5),11)]）を想定しており，一度危殆化したセンサでも新規センサと交換することで安全性を回復することができる．リンク以外にもセンサのストレージに対する暗号化方式として，Ma 等や Pietro 等によって DISH 方式[7] や POSH 方式[9] が提案されている．両方式ともに，配置された各センサは周囲のセンサの協力を得ることで，ストレージの暗号鍵の更新を行う．周囲のセンサの中に安全なセンサが存在する場合，鍵更新によって鍵の安全性を回復することができる．

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

WSNs の鍵共有方式にとって重要となることは，攻撃に対し Forward Secrecy（過去の秘密情報の秘匿）や Backward Secrecy（未来の秘密情報の秘匿），Self-Healing（安全性の自己治癒）の特性を満たすことである．しかし，3 つ全てを満たすことは難しく，既存方式の多くは満たしていない．また，全特性を満たす RoK 方式においても，一度危殆化したセンサの安全性は交換しない限り回復することはできない．我々は CSS2010 において，各センサが周りのセンサの協力を得て共有リンク鍵の更新を行うことにより，センサの交換なくとも上記 3 つの特性を全て満たす鍵共有方式を検討した．しかし，共有リンク鍵の自己治癒機能やマルチフェーズ WSNs への適用に対する考察が不十分であった．本稿では，鍵の更新方法，効率的なマルチフェーズ WSNs への適用方法についてさらなる検討を行った．また，数式モデルやシミュレーションプログラムによる評価によって安全性の確認を行った．

2. 準　　備

2.1 共通表記

以下に本稿で使用する共通表記を示す．

n	:	WSNs におけるセンサの総数
s_i	:	センサ i
ID_i	:	s_i の識別子
m	:	1 センサが持つリンクの平均数
r	:	ラウンド数
$K_{i,j}^r$	:	ラウンド r における s_i と s_j の共有リンク鍵
S_i^r	:	ラウンド r における s_i のシード
$c_{i_\ell}^r$	:	ラウンド r において s_i が受信した ℓ 個目の補助データ
G^r	:	ラウンド r における非危殆化センサ
Y^r	:	ラウンド r における回復していないセンサ
R^r	:	ラウンド r における攻撃者が侵入中のセンサ（$\|R^r\| = k$）
GL^r	:	ラウンド r における非危殆化リンク
RL^r	:	ラウンド r における危殆化リンク
q	:	大きな素数
$PRNG$	:	疑似乱数生成関数
H	:	ハッシュ関数 $H : \{0,1\}^* \rightarrow \{0,1\}^q$
$f(x,y)$	:	対称式である 2 変数多項式 $f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$

2.2 評価基準

本研究で用いる評価基準である接続確率と危殆化率について以下に示す．

接続確率（Availability）： 隣接するセンサ間で暗号に用いる鍵の合意に成功する確率のことである．接続確率が高いほど，センサ間で共有リンク鍵を構成できる可能性が高い．

危殆化率（Compromised-link(Red link) ratio）： WSNs 全体のリンク数と攻撃者によって危殆化されたリンクの割合を示す．共有リンク鍵の全構成要素を攻撃者に知られた時，その鍵を用いているリンクは危殆化されたリンクとなる．攻撃者によって WSNs にある全てのリンクが危殆化した際，危殆化率は 100%となる．

2.3 セキュリティ要件

本研究及び WSNs の鍵共有方式において必要要件となる 3 つの特性について示す．

Forward Secrecy: 現在の鍵から，過去の鍵を作ることができない特性である．Forward Secrecy を満たすことにより，攻撃者は現在の鍵から過去の鍵を構成し，過去の通信で利用された暗号データの解読などの攻撃を行うことができない．

Backward Secrecy: 現在の鍵から，未来の鍵を作ることができない特性である．Backward Secrecy を満たすことにより，現在の鍵から未来の鍵を構成し，現在以降の通信で利用される暗号データの解読などの攻撃ができない．

Self-Healing: 暗号鍵が危殆化した際，危殆化した鍵を自己治癒する特性である．Self-Healing を満たすことにより，一度鍵が危殆化しても安全な状態に回復することができる．

2.4 攻撃者モデル

本研究において，攻撃者（ADV）は既存研究[7)–9)] を参考とし，WSNs 内を自由に移動できる攻撃者（Mobile Adversary）を想定する．ADV の目的は可能な限り多くのセンサの秘密情報（秘密鍵や他の鍵の情報）を収集し，暗号化されたデータの解読に生かすことである．等間隔に時間を分けたラウンド毎に攻撃を行う．ADV は各ラウンド毎に k 個の非危殆化センサ（情報が漏洩していないセンサ）に移動・侵入し秘密情報を危殆化する．また，侵入したセンサの送受信を盗聴する．危殆化したセンサから取得したセンサの秘密情報は各攻撃者が共有し，暗号化通信の解読に利用することができる．さらに，ADV はネットワークトポロジ，危殆化したセンサや安全なセンサの位置を把握しているため非危殆化センサのみ攻撃することができる．ADV は可能な限り発見されずに WSNs 内に存在するために，センサの動作を妨げず，送受信メッセージの削除や遅延，偽造した情報の注入などは行わない．

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

3. 関連研究（POSH 方式[9]）

3.1 概　　要

POSH 方式は Pietro 等が提案したストレージ暗号化方式である．POSH 方式では，各センサが周囲のセンサと協力することでストレージの暗号化鍵更新を行う．

POSH 方式ではセンサの状態を以下の 3 種類に分類している．

危殆化中のセンサ（Red sensor）（R^r）： ラウンド r において ADV が侵入中のセンサを示す．秘密情報の安全性は回復することができない状態である．

回復待ちセンサ（Yellow sensor）（Y^r）： ラウンド $r'(r' < r)$ において危殆化されたセンサであり，安全性が回復していない状態のものを示す．ラウンド r において ADV が侵入中ではないが，秘密情報は全て漏洩している．非危殆化センサから補助データを受信することで秘密情報の安全性を回復できる．

非危殆化センサ（Green sensor）（G^r）： ラウンド r において ADV に秘密情報を知られていない安全な状態であるセンサである．一度も危殆化していないセンサ，または，安全性を回復したセンサを示す．

3.2 プロトコル

3.2.1 初 期 設 定

各センサ s_i がラウンド r においてストレージの暗号化に使用する秘密鍵を K_i^r とする．s_i はラウンド 1 において秘密鍵 K_i^1 と疑似乱数生成関数（$PRNG$）のシードを基地局と共有する．秘密鍵とシードは各センサ毎に異なるものを使用する．また，各センサは共有のハッシュ関数 H と $PRNG$ を所有する．

3.2.2 鍵　更　新

センサは $PRNG$ を用いてランダムに u 個の補助データの送信先を決める．次にランダムに u 個の補助データ c を生成し送信先に送付する．送信先のセンサは，受信した補助データを現在の鍵と同時にハッシュ関数にかけ，次のラウンドの鍵を生成する．ラウンド r における s_i の鍵更新は以下の通りである．

$$K_i^{r+1} = H(K_i^r || c_{i_1}^r || ... || c_{i_\ell}^r),\ r \geq 1 \tag{1}$$

この時，センサ s_i は ℓ 個補助データを受信していることを表す．この鍵更新において，非危殆化センサの補助データを鍵更新に利用することが可能であれば，Forward Secrecy，Backward Secrecy，Self-Healing の特性全てを満たすことができる．

4. 提 案 方 式

提案方式の目的は，POSH 方式のアイディアを利用して，ADV が存在する環境においてもセンサを交換することなく，WSNs のリンクの安全性を Self-Healing できる鍵共有方式の提案することである．提案方式では，ラウンド毎の鍵更新に周囲のセンサから補助データを収集し，現在の共有リンク鍵と組み合わせることで次ラウンドの鍵を生成する．また，補助データを用いて POST 方式[10] のようにシードの更新も行う．

各ラウンドにおいてセンサは POSH 方式と同様に 3 つの状態（Red（R^r），Yellow（Y^r），Green（G^r））に分類できる．また，リンクも以下のように分類することができる．

危殆化リンク（Red link）（RL^r）： ラウンド $r'(r' \leq r)$ によって攻撃され，ラウンド r において危殆化しているリンクである．ADV がいつでもリンク内の通信データを見ることができるため，安全性を回復する必要がある．

非危殆化リンク（Green link）（GL^r）： 一度も危殆化していないリンク，もしくは危殆化した状態から安全性を回復したリンクである．

4.1 プロトコル

4.1.1 初 期 設 定

サーバの設定: サーバは ID を生成し，配置前の各センサ s_i に ID_i を保存する．次に，$a_{ij} \in \{0,1\}^q$ を含む位数 q の有限体上の 2 変数多項式 $f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$ を 1 個生成する．$f(x,y)$ は t 次の対称多項式（$f(x,y) = f(y,x)$）とする．さらに，多項式に各センサが持つ ID を代入し $f(x, ID_i)$ を計算する．

センサの設定: $f(x, ID_i)$ は初期多項式として ID に対応するセンサ s_i に保存する．s_i は一方向性ハッシュ関数 H とセンサ毎に異なるシード S_i^r を利用した疑似乱数生成関数 $PRNG$ を利用することができる．

4.1.2 初期共有リンク鍵の生成

配置されたセンサ s_i は隣接するセンサ s_j と初期共有リンク鍵の生成を行う．s_i は所有している多項式 $f(x, ID_i)$ より，$f(ID_j, ID_i)$ を生成する．s_j は所有している多項式 $f(x, ID_j)$ より，s_i との共有リンク鍵となる $f(ID_i, ID_j) = f(ID_j, ID_i)$ を生成することができる．その結果，ラウンド 1 において，センサ si と s_j は共有リンク鍵 $K_{i,j}^1 = f(ID_i, ID_j) = f(ID_j, ID_i)$ を生成することができる．共有リンク鍵の生成後，各センサは多項式の係数を全て消去する．

4.1.3 共有リンク鍵とシードの更新

ラウンド 1 においてセンサ s_i と s_j は初期共有リンク鍵 $K_{i,j}^1$ を生成する．以降のラウン

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

ドでは共有リンク鍵と $PRNG$ のシードの更新を行う．ラウンド r の開始時，s_i は $PRNG$ を用いて m 個のランダム値（補助データ）を生成する．生成した補助データは共有リンク鍵を用いて暗号化し，各隣接センサ s_j に送信する．この時，送信する補助データは各隣接センサ毎に異なるものを使用する．r ラウンド終了時，現在の共有リンク鍵とリンク先と共有する補助データをハッシュ関数にかけ，以下のように $r+1$ ラウンドの鍵を生成する．

$$K_{i,j}^{r+1} = H(K_{i,j}^r || c_{i_\eta}^r || c_{j_\lambda}^r) \tag{2}$$

この時，$c_{i_\eta}^r$ は s_i が受信した η 個目の補助データ（s_j が送信した補助データ）を表し，$c_{j_\lambda}^r$ は s_j が受信した λ 個目の補助データ（s_i が送信した補助データ）を表す．鍵更新後，s_i と s_j は $K_{i,j}^r$ を消去する．

さらに，各センサは m 個の補助データ（受信した全ての補助データ）を用いて，$PRNG$ のシードを更新する．ラウンド r 終了時，s_i はシード S_i^r を以下のように更新する．

$$S_i^{r+1} = H(S_i^r || c_{i_1}^r || \cdots || c_{i_m}^r) \tag{3}$$

シード更新後，s_i は S_i^r を消去する．

4.2 リンクの状態遷移

リンクは以下の 2 ステップで自己治癒する．まず初めに，2 個の隣接しているセンサが回復する．そして次に，それらの間のリンクが回復する．

リンクを持つ 2 つのセンサのどちらかが危殆化センサ（Y^r，R^r）である場合，リンクは危殆化した状態（RL^r）となる．また，危殆化リンク RL^r で接続しているセンサのどちらかに ADV が侵入している場合，リンクの回復には少なくとも 2 ラウンドを必要とする．危殆化リンク RL^r で接続しているセンサがある時，両方が非危殆化センサ G^r であり，少なくともどちらか一方のセンサが送信した補助データが ADV に盗聴されない時，RL^r は非危殆化リンク GL^r となる．非危殆化リンク GL^r で接続している非危殆化センサが存在する時，少なくとも 1 個のセンサが危殆化した場合，リンクは危殆化する．後の図 5 にリンクの状態遷移図を示す．

4.3 具 体 例

プロトコルの補助データ送受信，共有リンク鍵更新，シード更新の動作例を示す．

(1) 補助データの送受信: 図 1 を例に補助データの送受信について説明する．s_1 と s_2 のリンクを例に挙げる．s_1 には 3 つの隣接センサ（s_2，s_3，s_4）が存在し，s_2 には 2 つの隣接センサ（s_1，s_6）が存在する．ラウンド r において，s_1 と s_2 の共有リンク鍵を $K_{1,2}^r$，s_1 のシードを S_1^r，s_1 のシードを S_2^r とする．

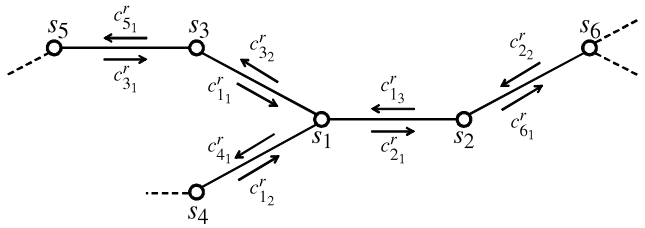

図 1 補助データの送信例

ラウンド r 開始時，各センサは補助データを送信する．例として，s_1 は補助データ $c_{2_1}^r$，$c_{3_2}^r$，$c_{4_1}^r$ を生成し，隣接センサである s_2，s_3，s_4 に送信する．

ラウンド r の間，各センサは隣接センサから補助データを受信する．例として，s_1 は $c_{1_3}^r$，$c_{1_1}^r$，$c_{1_2}^r$ を s_2，s_3，s_4 から受信する．ここで，$c_{1_\ell}^r$ はラウンド r において s_1 が受信した ℓ 個目の補助データであることを示す．この例では，最初に s_3 から $c_{1_1}^r$ を受信し，次に s_4 から $c_{1_2}^r$ を受信し，最後に s_2 から $c_{1_3}^r$ を受信したことになる．

(2) 共有リンク鍵の更新: ラウンド r 終了時，各センサは隣接センサと共有する補助データを用いて鍵更新を行う．また，受信した全補助データを用いて $PRNG$ のシードの更新を行う．例として，s_1 と s_2 は以下のように鍵更新を行う．

$$K_{1,2}^{r+1} = H(K_{1,2}^r || c_{1_3}^r || c_{2_1}^r) \tag{4}$$

鍵更新後，s_1 と s_2 は $K_{1,2}^r$ を消去する．

(3) シードの更新: さらに s_1 は以下のようにシードを更新する．

$$S_1^{r+1} = H(S_1^r || c_{1_1}^r || c_{1_2}^r || c_{1_3}^r) \tag{5}$$

シード更新後，s_1 は S_1^r を消去する．

WSNs では無線通信を行うため，あるセンサの通信は全ての隣接センサが受信できる．例えば，補助データ $c_{1_1}^r$ は s_1 と同様に s_5 も受信できる．この時，センサの状態が $s_3 \in G^r$，$s_5 \notin R^r$，$s_1 \in Y^r$ である場合，$c_{1_1}^r$ は ADV に盗聴されず s_1 は非危殆化センサへと回復することができる．しかしながら，センサが $s_3 \in G^r$, $s_5 \in R^r$，$s_1 \in Y^r$ である場合，補助データは $c_{1_1}^r$ は ADV（s_5）に盗聴され，s_1 は回復しない．

5. 評　　価

評価を行う目的は提案方式の ADV に対する耐性や可用性を示すことである．評価はシミュレーションプログラムと数式モデルを用いることによって，評価の正確さを向上させた．

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

5.1 シミュレーション評価

シミュレーション評価について以下に述べる．シミュレーションでは，シミュレーションプログラムを用いて，提案方式の ADV に対する耐性を示すため，危殆化リンク RL^r の比率（危殆化率）を評価した．

5.1.1 環 境 設 定

シミュレーションを行った際の環境を以下に示す．シミュレーションは Windows XP SP3 上で C 言語を用いて実行した．全てのシミュレーションは 1000 回繰り返して行い，シミュレーション結果は 1000 回の平均を取ったものとした．

想定した WSNs は以下の通りである．ネットワークトポロジはメッシュ型であり，ネットワークは球状の地形への配置を想定する．また，時間経過によるトポロジの変化は考えない．センサノード数 $n = 400$（20×20），各センサの隣接センサ数 $m = 4$，WSNs 全体のリンク数を 800 とする．ADV の数 k は 5，10，50，100 の場合を比較した．

攻撃モデルは 2 種類用意した．毎ラウンド連続して攻撃を行う ADV（Continuous Attacker Model）と一定期間（ラウンド 5〜14）攻撃を行う ADV（Temporary Attacker Model）に対して，提案方式の危殆化率を評価した．攻撃は一定間隔（ラウンド）毎に行い，1 ラウンド k 個の非危殆化センサ G^r を危殆化することができる．

5.1.2 シミュレーション評価結果

Continuous Attacker Model の結果を図 2，Temporary Attacker Model の結果を図 3 に示す．Continuous Attacker Model の場合，$k \geq 62$ の時に危殆化率は 100%となった．また，$k = 5$ の時 5.1%，$k = 10$ の時 10%，$k = 50$ の時 52%，$k = 100$ の時 100%となった．Temporary Attacker Model の場合，ADV が攻撃をやめると同時に危殆化リンクは減少し，3 ラウンドほどで WSNs 全体のリンクの安全性を回復することができた．1 度でも WSNs 全体のリンクが危殆化した場合，ADV が攻撃をやめたとしても回復することはない．

5.2 理 論 評 価

理論評価について述べる．理論評価では WSNs の状態遷移を表す理論式を用いて危殆化率の評価を行った．また，接続確率やメモリの評価についても述べる．

5.2.1 状 態 遷 移

WSNs の状態遷移および状態遷移の理論式について述べる．WSNs において状態が遷移するものはセンサとリンクである．センサの状態が決定し，その後リンクの状態が決定する．

センサの状態遷移: センサの状態は POSH 方式と同様に Green（安全），Yellow（危殆化・回復待ち），Red（ADV 侵入中）を用いる．また，遷移も同様に図 4 のように行われる．

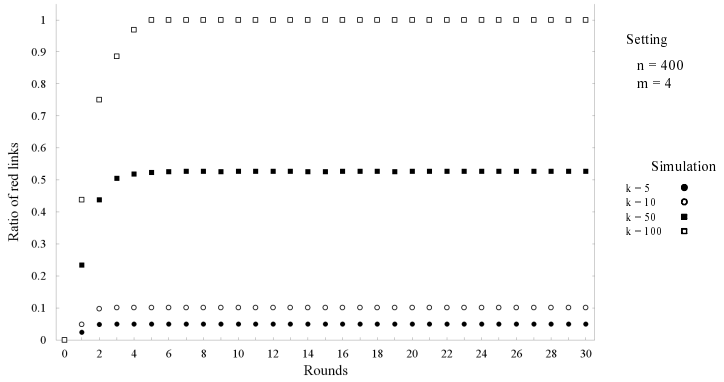

図 2 Continuous Attacker Model の結果

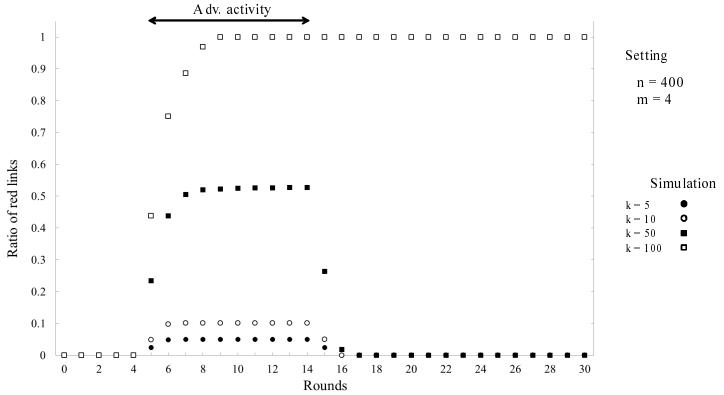

図 3 Temporary Attacker Model の結果

センサの状態遷移を求める際，補助データの送受信が重要となる．回復待ちセンサは非危殆化センサの補助データを受信しないと安全性を回復できない．また，非危殆化センサの補助データは非危殆化センサの隣接センサが危殆化している場合，ADV に盗聴されてしまう．2 ホップ先のセンサが少なくとも 1 つ危殆化センサ（盗聴者）である確率は $(1-(1-p_{R^r})^{m-1})$ と表せる．よって，回復待ちセンサが安全性を回復できない確率は以下のようになる．

$$Pr' = \sum_{i=0}^{m} \binom{m}{i} p_{G^r}^{i} (1 - p_{G^r})^{m-i} (1 - (1 - p_{R^r})^{m-1})^{i} \tag{6}$$

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

ここで，$p_{G^r} = |G^r|/(n-1)$, $p_{Y^r} = |Y^r|/(n-1)$，$p_{R^r} = |R^r|/(n-1)$ とする．p_{G^r}，p_{Y^r}，p_{R^r} はそれぞれ WSNs における G^r，Y^r，R^r の割合を示す．ラウンド r において非危殆化センサ数の期待値は以下のように表すことができる．

$$E[|G^{r+1}|] = |G^r| + (1 - Pr')|Y^r| - |R^r| \tag{7}$$

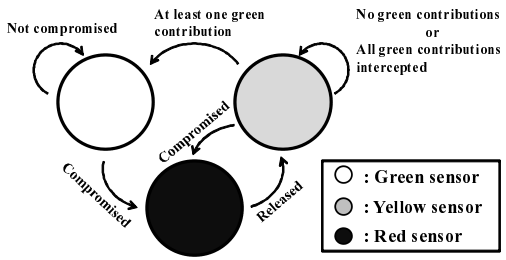

図 4 センサの状態遷移図

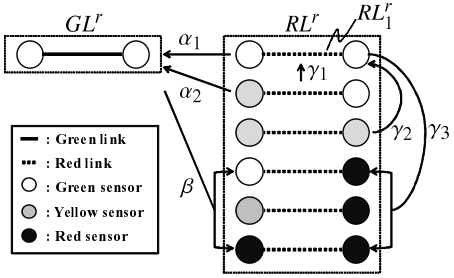

図 5 リンクの状態遷移図

5.2.2 リンクの状態遷移

提案方式においてリンクの状態遷移は図 5 のように行われる．図 5 では安全なリンクの数を分析するために必要な遷移だけを表している．

図 5 から，リンクの状態は 7 種類に分類することができる．また，α_1, α_2, β, γ_1, γ_2，γ_3 はそれぞれ遷移するリンクの数を表す．遷移を行わないリンクも存在する．$RL_1^r \subset RL^r$ となる RL_1^r は非危殆化センサ間のリンクが危殆化している状態を示す．

GL^{r+1} の期待値: ラウンド $r+1$ の非危殆化リンク GL の期待値を以下に示す．

$$E[|GL^{r+1}|] = |GL^r| + \alpha_1 + \alpha_2 - \beta, \tag{8}$$

$\alpha_1 = (1-(1-(1-p_{R^r})^{m-1})^2)|RL_1^r|$，$\alpha_2 = (1-Pr')|Y^r|p_{\alpha_2}$，$\beta = |R^r|p_\beta$ となる．

α_1 は RL_1^r から GL^r に遷移するリンク数を表す．RL_1^r の状態の時，2 つの非危殆化センサの一方の全隣接センサに盗聴者がいない場合，α_1 の遷移が起こる．α_2 は非危殆化センサと回復待ちセンサが接続するリンクが GL^r に遷移するリンク数を表す．α_2 の理論式で用いられる p_{α_2} は隣接センサの少なくとも 1 個が安全であり，その非危殆化センサの隣接センサ中に危殆化センサ（ADV）が存在しない確率である．β は GL^r から RL^r に遷移するリンク数を表す．GL^r の状態の時，ADV がセンサを危殆化すると β の遷移が起こる．β の理論式で用いられる p_β は少なくとも 1 つの非危殆化センサが危殆化する確率である．p_{α_2}，p_β の式は以下の通りである．

$$p_{\alpha_2} = \sum_{i=0}^{m} \binom{m}{i} (p_{G^r}(1-p_{R^r})^{m-1})^i (1 - p_{G^r}(1-p_{R^r})^{m-1})^{m-i} i \tag{9}$$

$$p_\beta = \sum_{i=0}^{m} \binom{m}{i} (p_{G^r}\mu)^i (1 - p_{G^r}\mu)^{m-i} i \tag{10}$$

$\mu = |GL^r|/(|GL^r| + |RL_1^r|)$ であり，非危殆化センサ間のリンクが GL^r である割合を示す．

RL_1^{r+1} の期待値: ラウンド $r+1$ の非危殆化センサ間の危殆化リンク RL_1 の期待値は以下のように表すことができる．

$$E[|RL_1^{r+1}|] = |RL_1^r| - \alpha_1 + \gamma_1 + \gamma_2 - \gamma_3 \tag{11}$$

ここで，$\gamma_1 = (1-Pr')|Y^r|p_{\gamma_1}$，$\gamma_2 = (1-Pr')|Y^r|p_{\gamma_2}$，$\gamma_3 = |R^r|p_{\gamma_3}$ となる．

γ_1 は RL^r から RL_1^r へと遷移するリンク数を表す．回復するセンサのリンク先が非危殆化センサであり，かつその非危殆化センサの補助データを ADV に盗聴される際に γ_1 の遷移が起こる．p_{γ_1} はリンク先の状態が安全であり，かつそのセンサの補助データを盗聴する ADV がそのセンサの隣接センサに存在する確率を示す．γ_2 は γ_1 と同様に RL^r から RL_1^r へと遷移するリンク数を表す．両センサの状態が回復する際に γ_2 の遷移が起こる．両センサ共に ADV に送信する補助データが推測されてしまうためこの遷移が起こる．p_{γ_2} はリンク先が回復するセンサである確率である．γ_3 は RL_1^r から RL^r に遷移するリンク数を表す．RL_1^r の状態時，少なくともどちらかのセンサが ADV によって危殆化すると γ_3 の遷移が起こる．p_{γ_3} は非危殆化センサのリンクが RL_1^r である確率を示す．p_{γ_1}，p_{γ_2}，p_{γ_3} の式は以下の通りである．

$$p_{\gamma_1} = \sum_{i=0}^{m} \binom{m}{i} (p_{G^r}(1-(1-p_{R^r})^{m-1}))^i (1 - p_{G^r}(1-(1-p_{R^r})^{m-1}))^{m-i} i \tag{12}$$

$$p_{\gamma_2} = \sum_{i=0}^{m} \binom{m}{i} ((1-Pr')p_{Y^r})^i (1 - (1-Pr')p_{Y^r})^{m-i} i \tag{13}$$

$$p_{\gamma_3} = \sum_{i=0}^{m} \binom{m}{i} (p_{G^r}(1-\mu))^i (1 - p_{G^r}(1-\mu))^{m-i} i \tag{14}$$

上記と同様に，$\mu = |GL^r|/(|GL^r| + |RL_1^r|)$ である．

5.2.3 理論評価結果

シミュレーション結果と理論式で得た結果の比較グラフを図 6 に示す．理論式の結果はシミュレーションで得た結果とほぼ一致し，評価の正確性を示せた．

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

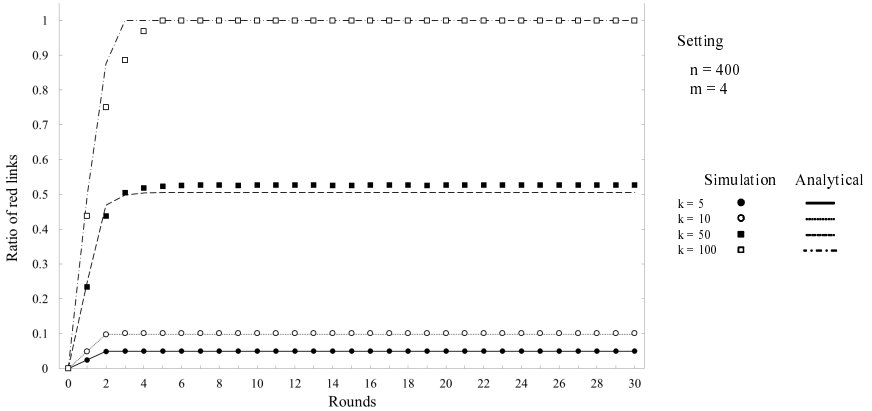

図 6 理論値と実験値の比較

5.3 接続確率の評価

ラウンド 1 において，センサ s_i は多項式 $f(x, ID_i)$ を用いて，隣接センサ s_j と $K_{i,j}^r = f(ID_j, ID_i)$ で鍵共有を行う．そして，その後のラウンドではラウンド 1 の鍵を更新したものを用いるため，提案方式の接続確率は 100%となる．

5.4 その他の評価

提案方式を適用した際の計算量，通信量，ストレージについて述べる．R と H を PRNG とハッシュの計算コストとし，補助データ，ID，ハッシュの出力，多項式の係数のサイズを $|2^q|$ とする．

1 ラウンドの各センサの計算量は $mR + (m+1)H$ となる．ラウンド 1 においては，多項式を用いて共有鍵の生成を行うため，その分の計算量が必要となる．1 ラウンドの各センサの通信コストは送受信を合わせて $2m|2^q|$ となる．ラウンド 1 においては，ID の交換をするために必要な通信量がかかる．ラウンド 1 において必要なストレージの量は多項式の係数，シード，ID を合わせて $(t+3)|2^q|$ となる．初期共有リンク鍵生成後はセンサ s_i は多項式の係数を消去する．また，共有リンク鍵として $m|2^q|$，補助データの送受信に $2m|2^q|$ のストレージが必要となる．そのため，ラウンド 1 より後のラウンドでは $(t+1-3m)|2^q|$ のメモリを削減できる．したがって，$(t+1) \geq 3m$ であれば必要な 1 ラウンド目以降に余分なストレージを確保することはない．提案方式は，以上のように効率的であり，限られた演算性能（メモリ，CPU）と電源容量のセンサで構成される WSNs に適当であるといえる．

6. 考　　察

6.1 既存方式との比較

提案方式と既存方式である RoK 方式[1] との比較結果を図 7 に示す．既存方式の中で，RoK 方式が最もシンプルかつ計量な演算量で Self-Healing を行える方式であるため，今回比較対象とした．攻撃者数 $k = 5$ とし，RoK 方式のセンサの平均寿命（平均生存期間）は 50 ラウンドとしている．攻撃者は 1 ラウンド毎に 5 個のセンサを危殆化する．また，RoK 方式のセンサ交換と提案方式の補助データ送受信のタイミングは 10 ラウンド毎である（RoK 方式の 1Generation=10rounds を参考とし，RoK 方式と比較するため，補助データの送受信のタイミングを 10 ラウンド毎とした.）．この結果，危殆化率は提案方式の方が低く抑えられ，攻撃者に対してより強い耐性を持つことが分かった．RoK 方式では，センサが危殆化するとそのセンサと全く関係のないリンクまで危殆化してしまう可能性がある．このことが，危殆化率が上昇した原因だと考えられる．

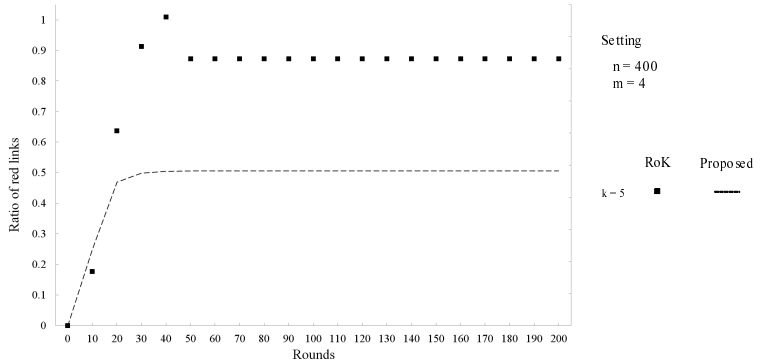

図 7 RoK 方式との比較

6.2 マルチフェーズ WSNs への適用

マルチフェーズ WSNs とはセンサを追加投入することで，接続性維持とセキュリティ向上を図る WSNs のことである．通常の WSNs では，攻撃による危殆化や電池切れの影響により安全なリンク数が時間経過とともに減少してしまう．一方，マルチフェーズ WSN 方式では，新たにセンサを投入することで，安全性・接続率の維持が可能である．提案方式ではセンサの追加投入がなくとも Self-Healing が可能である．しかしながら，長期利用という観点のため，マルチフェーズ WSNs への適用を試みた．マルチフェーズ WSNs に適用する場

Vol.2011-DPS-146 No.31
Vol.2011-CSEC-52 No.31
2011/3/11

合，新規センサとの鍵共有が困難となる．そこで，配置後すぐに鍵共有を行わず，補助データを交換後に鍵共有を行う単純な方式を提案する．

ラウンド r の開始時，配置される新規センサ s_i は多項式を持たないものとする．配置後の s_i は m 個の隣接センサ s_j にそれぞれ補助データを送信する．同様に s_j は補助データを s_i に返信する．この時，補助データの送受信には暗号化を用いることはできない．s_i と s_j は式 (2) のように共有リンク鍵の生成を行う．ここで，$K_{i,j}$ は 1 とする．s_i は鍵生成を行い，$r+1$ ラウンドでは m 個の共有リンク鍵を生成できる．さらに，鍵共有後 s_i は式 (3) のようにシードの更新を行う．

シミュレーション結果を図 8 に示す．図 8 の WSNs ではラウンド 1 に n 個のセンサを配置する．また，ガウス分布に従って，センサの使用期限をランダムに設定した．RoK 方式との比較と同様に，平均 50 ラウンドとなるようにガウス分布を設定した．この時，標準偏差は 16.67，センサの最大使用期限（生存期間）は 100 であり，RoK 方式[1] や RPoK 方式 IMO10 と同様に設定した．センサは使用期限が過ぎたら，随時新規センサと交換される．ただし，センサ同士が補助データを送受信するタイミングは 1 ラウンド毎とした．

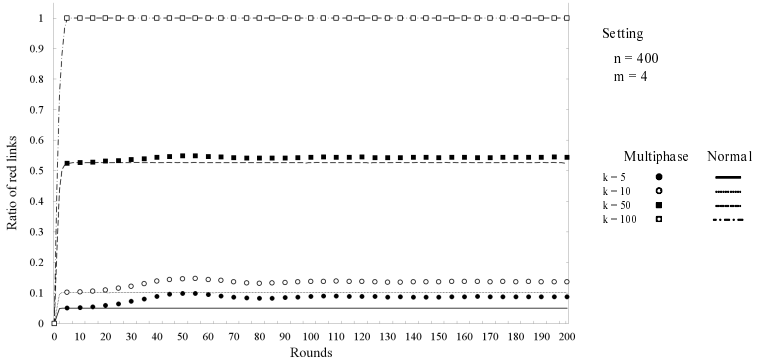

図 8 マルチフェーズ WSNs のシミュレーション結果

図 8 では通常の提案方式（Normal）よりもマルチフェーズに適用した方が危殆化率が高くなることがわかる．これは，これまで危殆化していなかったリンクが，センサを新しく配置することによって危殆化する恐れがあるためである（ここでは，新規センサのリンクが危殆化する確率は高くなるため，新規センサのリンクは全て危殆化するとして評価を行った.）．以上のように提案方式はマルチフェーズ WSNs への適用することができる．しかしながら，拡張性・危殆化率の面で問題点もあるため改良の必要がある．

7. おわりに

本稿では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を行った．提案方式は攻撃者に対して，ラウンド毎にセンサ同士が協力して鍵更新を行うことで，Forward Secrecy，Backward Secrecy，Self-Healing の 3 つの特性を満たすことができる．また，シミュレーションプログラムを用いた実験値と数式モデルを用いた理論値の評価において，提案方式が攻撃者に対して非常に耐性を持つことと評価の正確性を示した．また，センサ間の接続確率は 100%にすることができることを示した．考察として，既存方式との比較と提案方式をマルチフェーズ WSNs への適用方法を述べた．

参考文献

1) C.Castelluccia and A.Spognardi. RoK: A robust key pre-distribution protocol for multi-phase wireless sensor networks. In *SecureComm2007*, pages 351–360, 2007.
2) H.Chan, A.Perrig, and D.Song. Random key predistribution schemes for sensor networks. In *S&P'03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 197–213, 2003.
3) L.Eschenauer and V.D.Gligor. A key-management scheme for distributed sensor networks. In *CCS'02*, pages 41–47, 2002.
4) H. Ito, A. Miyaji, and K. Omote. RPoK: A strongly resilient polynomial-based random key pre-distribution scheme for multiphase wireless sensor networks. In *Globecom*, pages 1–5, 2010.
5) K. Kalkan, S. Yilmaz, O.Z. Yilmaz, and A. Levi. A highly resilient and zone-based key predistribution protocol for multiphase wireless sensor networks. In *Q2SWinet'09*, pages 29–36, 2009.
6) D.Liu, P.Ning, and R.Li. Establishing pairwise keys in distributed sensor networks. In *ACM Trans. Inf. Syst. Secur*, Vol. 8, No. 1, pages 41–77, 2005.
7) D. Ma, and G. Tsudik. DISH: Distributed self-healing. In *SSS'08*, pages 47–62, 2008.
8) R. Ostrovsky, and M. Yung. How to withstand mobile virus attacks. In *PODC*, pages 51–59, 2007.
9) R.D. Pietro, D. Ma, C. Soriente, and G. Tsudik. POSH: Proactive co-operative self-healing in unattended wireless sensor networks. In *SRDS'08*, pages 185–194, 2008.
10) R.D.Pietro, G.Oligeri, C.Soriente, and G.Tsudik. Intrusion-Resilience in Mobile Unattended WSNs. In *INFOCOM*, pages 2303–2311, 2010.
11) O.Z. Yilmaz, A. Levi, and E. Savas. Multiphase deployment models for fast self healing in wireless sensor networks. In *SECRYPT*, pages 136–144, 2008.