Vol.2015-CSEC-69 No.4
Vol.2015-IOT-29 No.4
2015/5/21

クラスタツリー型のセンサネットワークにおける安全で高効率な鍵共有方式

後藤慎一[†1]　岩村惠市[†2]

センサネットワークの構成の一つに複数のノードを集めてクラスタ化を行い，接続を階層化するクラスタツリー型がある．このシステムに暗号通信を考慮した場合，既存の暗号鍵共有法では，クラスタ内のノードのリーダー(以下，CH と呼ぶ)を解析すればクラスタ内の全ノードの鍵情報が漏えいする問題や，全ノードが CH になる可能性がある場合に，全ノードに比較的大きな記憶容量を持たせなければならないという問題が生じる．
本論文では秘密分散法を用いて，クラスタツリー型のセンサネットワークにおいて CH とクラスタ内の全ノードと鍵共有でき，なおかつ以下の特徴を持つ鍵共有方式を各々提案する．
(1)　CH が解析されても鍵情報が全く漏えいしない情報量的安全性をもつ鍵共有方式
(2)　CH はクラスタ内の鍵情報を保存せず，自分の鍵のみを管理すればよい計算量的安全性をもつ鍵共有方式

Secure and efficient key sharing in clustered sensor networks

SHINICHI GOTO[†1]　KEIICHI IWAMURA[†2]

Wireless sensor network is a form of ad-hoc networks for the purpose of information monitoring. This system consists of sensor nodes and a base station. Sensor nodes send sensing information such as temperature or humidity to their base station directly or indirectly through multi-hop routing.
Sensor nodes are not tamper resistant due to cost factors. Therefore, high-performance CPU is not used in sensor nodes. So, it's difficult to conduct complicated calculations like in the public key encryption. Additionally, in the sensor node, memory capacity is low. So, we should have to minimize the data. Moreover, sensor nodes have low capacity battery. Therefore, efficient energy consumption is important consideration point. Clustered networks are composed of a group of nodes. Each cluster autonomously chooses a cluster leader named the cluster head. In each cluster, the cluster head is important factor, which receives some environmental data from ordinary nodes in its cluster. This data is then sent to the base station. In case of ordinary node, the average communication distance can be shortened using multi-hop cluster communication in this system. So, it can decrease energy consumption. But, in these networks, cluster head is unchanged. So, cluster head consume energy more quickly than others.
In this paper, we propose a two suitable key sharing scheme in clustered sensor networks using secret sharing. First, our method reduces memory capacity to share keys and can share keys with any other node. Additionally, it prevents an attacker from obtaining other link keys.

1. はじめに

無線で接続出来る端末のみで構成されるアドホックネットワークの一種として，センサネットワークがある．センサネットワークはセンサノードと基地局で構成されていて，センサノードは，温度や電力，湿度などの種々の情報を監視し収集し，集めた情報を直接，もしくは他のノードにマルチホップ通信を行うことで基地局へデータを送信する．用途としては，軍事目的から一般消費者をターゲットとした民生用まで多岐にわたり，新たな通信インフラとして期待されている．

センサノードの特徴について述べる．まず，センサノードは安価に作る必要があるために簡易な構造をしている．よって耐タンパー性に乏しく，高性能な CPU も使われていない．このことにより攻撃者がノードを盗難して解析することで内部情報を容易に得ることが出来る．また，公開鍵暗号方式のような高度な計算処理を行うことに適していない．加えて，メモリも小さいものであるため，記憶する情報を少なくする必要がある．さらに，バッテリーも低容量であるために効率的なエネルギーの消費が求められている．

センサノードのエネルギー消費を効率的にするために，色々な手法が研究されてきた．まず，基地局と各ノードが直接通信を行うという手法では遠くのノードが電力を大きく消費してしまうため，他のノードよりも早く電池切れになる問題がある．それに対して，ノードが観測したデータを基地局に近いノードに送信しそれを転送していく手法がある．送信電力は通信相手の距離が短いほど小さくなるため，近くのノードとの通信では消費エネルギーを小さくできる．しかしこの場合、基地局に近いノードほど転送量が増えるため，基地局に近いノードが先に電池切れになってしまう問題がある．このデータを転送する接続トポロジーとして，複数のノードを集めてクラスタ化を行い，接続を階層化するクラスタツリー型トポロジーと呼ばれる手法が提案されている．この手法はノードをいくつかのグループ（クラスタ）にわけて，そのクラスタ内でノードのリーダー(クラスタヘッド，以降 CH)を決定する．各クラスタのノ

†1 東京理科大学工学研究科電気工学専攻
†2 東京理科大学

ードはデータを CH に転送し，CH はそのデータを基地局へ転送する．しかしこの方法も CH となったノードは転送量が増えるため他のノードより早く電池切れになるという問題が解決されていない. そこで直接 BS と通信を行う CH を順番に変えていく手法，LEACH[1][2]が考案された．

LEACH(Low-Energy-Adaptive-Clustering-Hierarchy)は 1 つのノードが CH となっている期間をラウンドと呼び，各ノードが順番に CH になることを宣言し，基地局の命令なしに自立的にクラスタを編成する．最大の特徴は一定の周期ごとに全てのノードが CH になるようにする点である．このことにより CH による消費エネルギーの偏りを全てのノードに平均化し，ネットワークの寿命を長くすることができる．

しかしこのプロトコルの原案はセキュリティを考慮していない．そこで，LEACH に対するセキュリティ対策に関する研究として, SecLEACH[3]や MS-LEACH[4]が発案された. SecLEACH では LEACH に対してランダム鍵配布方式[5]を用いることで暗号通信を実現している．しかしランダム鍵配布方式の欠点である，鍵共有ができないノードが存在してしまう点と，多くの鍵 ID を知らせる必要がある点によりエネルギー消費が大きなものとなっている. また，もしノードが盗難された場合に他のリンク間の鍵も漏洩する危険性がありセキュリティ面で不完全な部分がある．また,MS-LEACH ではノードの鍵共有をする際に，LEAP の pairwise key を用いて暗号通信を実現している. しかしこの方式では初期鍵を消去するまでに初期鍵を盗難された場合に，ノードの ID がわかれば pairwise key を生成出来るため他の全ノードが漏洩するという欠点を抱えている．LEAP については次章の 2.3 でも記述する．

一方，CH のように基地局と直接通信を行うノードが存在する場合，暗号通信のために，Kerberos[6]などの既存の鍵共有法を用いることが出来る．Kerberos を用いれば，正当なノード間で必ず鍵共有ができ, BS がランダムに鍵を設定するならば安全性も確率できる．しかし，LEACH をはじめとするクラスタツリー型のセンサネットワークにおける最大の問題は，一般に CH はクラスタ内の全ノードと暗号通信を行うため全ノードの鍵を保持しており，CH を解析すればクラスタ内の全ノードの鍵情報が漏えいするということである．また，CH となるノードはクラスタ内の全ノードの鍵情報を保有する必要があるため，比較的大きな記憶容量が必要である．よって，LEACH のように全ノードが CH になる可能性がある場合，全ノードに比較的大きな記憶容量を持たせなければならないという問題が発生する．

そこで本論文では秘密分散法を用いて，クラスタツリー型のセンサネットワークにおいて CH とクラスタ内の全ノードと鍵共有でき，かつ以下を実現する方式を提案する．

(1) CH が解析されても鍵情報が漏えいしない情報量的安全性をもつ鍵共有方式を提案する．すなわち，この方式は CH を解析しても鍵情報に関して何の情報も得られないという従来にない特徴を実現する．
(2) CH はクラスタ内の鍵情報を保存する必要がなく, 自分の鍵のみを管理していればよい鍵共有方式を提案する．これによって，全ノードは CH になった場合に備えた比較的大きな記憶容量を不要にする. ただしこの場合, CH が解析された場合の安全性は情報量的安全性から計算量的安全性になる．

以上より，必要に応じて最適な手法を選ぶことができる. すなわち，安全性を重視し，比較的大きな記憶容量を許容する場合は(1)を実現する方式を選択でき，計算量的安全性で十分であるが，記憶容量を削減したい場合は，(2)を実現する方式を選択すればよい．

本論文の構成は，まず 2 章においてクラスタツリー型センサネットワークの例として LEACH プロトコルの詳細について述べ，関連研究として LEACH に対して用いられた鍵共有法であるランダム鍵配布方式と LEAP[7]についてその概要を説明する. まず 3 章において, Kerberos を LEACH に適用した場合について示し, その問題点を明らかにする。次に，4 章において Shamir の秘密分散法を LEACH に適用した場合について示し，それが上記(1)を実現することを示す。5 章において高橋らによって提案された非対称秘密分散方式を LEACH に適用する場合を示し，それが(2)を実現することを示す．そして最後に従来方式と各提案方式に対する安全や効率に関する評価を行う．

2. 従来研究

2.1 LEACH

LEACH(Low Energy Adaptive Clustering Hierarchy)とはクラスタを構成し，クラスタ内のノードのリーダーである CH を周期的に変え，ノードが消費するエネルギーを平均化することを試みる方式である．CH は近隣ノードが観測したデータを受信し，集めるだけでなく自身も情報を観測し，データを送信するために，電力消費量が他のノードよりも多い．このことが引き起こす消費電力の偏りの対策として, LEACH では CH は周期的に全てのノードが担当する. それにより電力消費の集中による電池切れを防ぐ役割を果たす．基本的な LEACH では 2 ホップを想定し，前提として基地局は十分なリソースを有しており，センサノードはリソースが小さい．また全てのセンサノードは基地局と直接通信することが可能であると仮定する．

LEACH は setup phase と steady-state phase の二つの段階で構成されている．setup phase では，各ノードが乱数を用いて CH になるかどうかを決定する．CH になるノードは自

Vol.2015-CSEC-69 No.4
Vol.2015-IOT-29 No.4
2015/5/21

分が CH であることを伝えるメッセージを各ノードにブロードキャストする．それを受信した各ノードは，信号の強さから最も近い CH を選択し，そこのクラスタメンバになることを CH へ伝達する．この過程が完了したら，CH はクラスタメンバに対して後の steady-state phase の通信のための TDMA スケジュールを割り当て，各メンバに送信する．steady-state phase では割り当てた TDMA スケジュールに基づいて観測データの転送を行う．各ノードは自分が所属する CH にデータを送信する．CH は複数のメンバから受信したデータを結合することで送信情報を圧縮する．CH は一つに結合したデータを基地局へ送信する．なお，setup phase，steady-state phase を合わせたものを 1 ラウンドと定義する．

2.2 ランダム鍵配布方式

ランダム鍵配布方式では，まず鍵の集合である鍵プールから鍵(要素鍵)を各ノードに無作為に持たせる．要素鍵には鍵 ID が付けられている．CH でなく，近くの CH と通信可能なノードを通常ノードと定義する．通信をする手順としては，まず CH が自分の持つ鍵 ID を通常ノードに知らせる．通常ノードはその中から共通した鍵の ID を CH に知らせる．その後通常ノードはその共通した鍵からリンク鍵を生成し，それを暗号化通信における共通鍵として用いて暗号化通信を行う．このように要素鍵自体を相手に知らせることなく，共通鍵を決めることができる．

2.3 LEAP

LEAP(Localized Encryption and Authentication Protocol)とはセンサネットワークを考慮して作られた鍵管理プロトコルの一つである．以下にその概要を示す．

LEAP では，各ノードに 4 つの鍵を持たせることを目的としている．1 つは基地局と共有する通 Individual Key，2 つ目にネットワークの全てのノードと共有する Group Key，3 つ目に近隣ノード全体で共有する Cluster Key，最後に近隣ノードと一対一で共有する Pairwise Key である．この 4 つの鍵の内，Individual Key と Group Key はノードに事前に格納しておく．今回は Pairwise Key の共有がメインテーマであるためその共有法を以下に示す．

Pairwise Key：まず，初期鍵 K_i を管理者が作成する．ノード u は自分の ID を用いてマスター鍵 $Ku = f_{Ki}(u)$ を作成する．ここで，$f_K(a)$とは K とaを入力とした擬似乱数関数のことである．その後，近隣ノードを HELLO メッセージを送信して探し，近隣ノード v から ACK メッセージが返ってきたらノード u は v の ID と Kv を知ることが出来る．これを用いて $K_{UV} = f_{KV}(u)$ を得る．これが Pairwise Key である．

3. 提案方式 1

以下に Kerberos を LEACH に適用した場合について示す．

3.1 Kerberos

Kerberos は共通鍵暗号を用いた認証プロトコルの一つである．以下にその概要を示す．Kerberos は鍵管理センターを用いて認証を行う方式である．よって，BS を鍵管理センターとすれば，安全に CH と通常ノードの正当性とその間の共通鍵を設定できる．前提として，鍵管理センターはクライアントとサーバーの鍵を知っていて，かつ鍵管理センターは信頼のおけるものとする．

はじめに，クライアントが認証を行いたいときに鍵管理センターに認証リクエストを送る．リクエストを受け取った鍵管理センターはクライアントにチケットとセッション鍵をクライアントの持つ鍵で暗号化し送る．チケットとは，クライアントの情報とセッション鍵を含んだものである．チケットはサーバーの持つ鍵で暗号化されている．チケットとセッション鍵を受け取ったクライアントは自分の持つ鍵を用いて復号を行い，セッション鍵を得る．その後クライアントはサーバーにチケットを送る．サーバーは送られてきたチケットを自分のもつサーバー鍵で復号し，クライアントの情報とセッション鍵を得るという手順になっている．このように Kerberos では，鍵管理センターを用いることで，クライアントとサーバーが相互認証を安全に行うことが可能である．

3.2 LEACH への適用

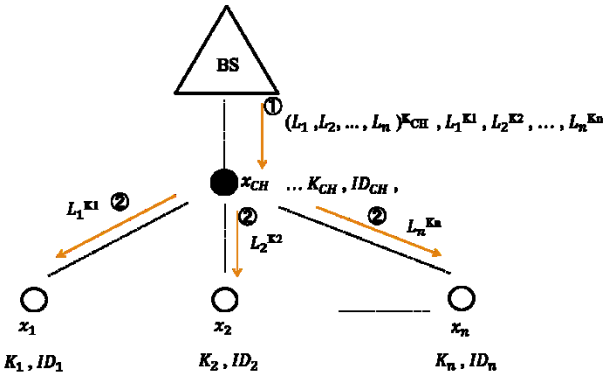

図 1.提案方式 1 の鍵共有方式

図 1 に CH(親ノード)●，子ノード○，基地局(Base Station)△をモデルとして，提案方式 1 の鍵共有方法について示す．まず，前提として各ノードに予め固有鍵($K_{CH}, K_1, K_{2,\ldots,}K_{n,}$)，ノード ID($ID_{CH}, ID_1\ ID_2\ , ID_{3,\ \ldots\ ,}ID_{n,}$)を持たせておく．これからリンク鍵($L_{1\ ,}\ L_{2\ ,}\ L_n$)を暗号通信用の鍵として以下の手順で共有を行う．

① まずノード ID を BS へ知らせる．そこから基地局は各ノードが暗号通信に用いるためのリンク鍵($L_{1\ ,}\ L_{2\ ,\ \ldots\ ,}\ L_n$)を各ノードの固有鍵($K_1, K_{2,\ \ldots\ ,}K_{n,}$)で暗号化する($L_1^{K1}$，$L_2^{K2}$，…，$L_n^{Kn}$)．更に，各ノードのリンク鍵

$(L_1, L_2, \ldots, L_n)$を CH の固有鍵で暗号化する$\{(L_1, L_2, \ldots, L_n)^{K_{CH}}\}$．暗号化の後に，基地局が CH へこれらを送信する．

② 暗号化されたリンク鍵を受信した CH は，自身の固有鍵で各ノードのリンク鍵を復号する，そして，各ノードにそれぞれの固有鍵で暗号化されたリンク鍵を送信する．

③ 各ノードは CH から送られてきた暗号化されたリンク鍵を自身の持つ固有鍵で復号し，リンク鍵を手に入れる．

3.3 評価・考察

Kerberos を LEACH に適用した場合の鍵共有方式の評価を行う．この方式を用いれば，鍵共有を確実にすることが出来，かつ暗号通信用の鍵を各ノードの固有鍵で暗号化して送信しているため，安全に配布することが出来る．また，もし子ノードを盗難された場合でも，そこから漏えいするのはそのノードの固有鍵と暗号通信用の鍵のみであり，他のノードに影響を及ぼさない．

しかし，もし CH を盗難された場合は，CH はクラスタ内の全てのセッション鍵を持っているため，クラスタ内の全てのセッション鍵が漏えいするという欠点がある．また，CH は各ノードに対応したセッション鍵を持つ必要があるために，CH が持つ鍵数は子ノードの数に応じて増加していく欠点がある．よって、この方式は著者らが知る限り今まで提案されていないが，最初にあげた 2 つの特徴を実現しないため、提案方式としているが比較のための方式である。

4. 提案方式２

4.1 Shamir の秘密分散法

提案方式 2 は鍵共有方式として Shamir の秘密分散法を用いる。Shamir の秘密分散法は以下の特徴を満たす。

・一つのデータを複数台のサーバーに分散し、閾値未満の数の分散情報が破損した場合でも元の情報を復元出来る．

・各サーバーに分散されている分散情報を閾値以上の数を集めない限り元の秘密情報を復元することができない．

今回の提案方式は，クラスタツリー型のセンサネットワークに Shamir の閾値秘密分散法[8]を用いて鍵共有方式を行うものである。

4.2 LEACH への適用

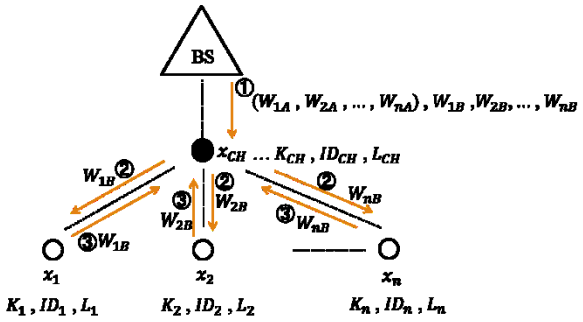

図 2.提案方式 2 の鍵共有方式

図 1 に CH(親ノード)●, 子ノード○, 基地局(Base Station)△をモデルとして, 提案方式 2 の鍵共有方法について示す．まず, 前提として各ノードに予め固有鍵($K_{CH}, K_1, K_2, \ldots, K_n$), ノード ID($ID_{CH}, ID_1 ID_2, ID_3, \ldots, ID_n$), リンク鍵($L_{CH}, L_1, L_2, L_n$)を持たせておく．これから，ノードのリンク鍵を秘密情報とし，以下の鍵共有を行う．まずノード ID を BS へ知らせる．そこから基地局は各ノードのリンク鍵(L_{CH}, L_1, L_2, L_n)をそれぞれ秘密情報とし, (2,2)の秘密分散を用いて分散情報(W_{1A}, W_{1B}), (W_{2A}, W_{2B}), …, (W_{nA}, W_{nB})を生成する．その後の手順は以下のようになる．

① 各ノードの片方の分散情報$W_{1A}, W_{2A}, \ldots, W_{nA}$を CH の固有鍵 K_{CH} で暗号化したものともう片方の各ノードの分散情報$W_{1B}, W_{2B}, \ldots, W_{nB}$ を CH へ送信する．

② CH は暗号化された分散情報$W_{1A}, W_{2A}, \ldots, W_{nA}$を自身の持つ固有鍵 K_{CH} で復号し，もう片方の分散情報$W_{1B}, W_{2B}, \ldots, W_{nB}$を対応する各ノードへ送信する．このとき CH は$W_{1B}, W_{2B}, \ldots, W_{nB}$を保持しない．

③ 各ノードは送られてきた分散情報を鍵共有する際に CH へ送信する．その後，CH は各ノードから送られてきた分散情報と自身の持つもう一方の分散情報を用いてリンク鍵 L_{CH}, L_1, L_2, L_n を生成する．以上の手順で提案方式 2 では鍵共有を行う．

4.3 評価・考察

Shamir の秘密分散法を用いた提案方式 2 について分析を行う．まず利点としては，この方式を用いた場合 CH は片方の分散情報しか保持していない．よって，もし CH を盗難された場合でも暗号通信用のリンク鍵を知るためには，それに対応する子ノードも盗難する必要がある。よって、CH が盗難されてもリンク鍵が漏洩することはない．また，Shamir の(2,2)秘密分散法は 1 つの分散情報から秘密情報が全く漏洩しないことを証明されているため，情報量的安全性をもつ．

しかし，CH は各ノードに対応した分散情報を持つ必要があるために，CH が持つ鍵数は子ノードの数に比例して増加していく欠点は提案方式 1 と同様である．

提案方式 2 を従来方式と比較する．SecLEACH は CH と

通常ノード間の鍵共有が確率的なものであり，鍵が共有できない場合がある．それに対して，提案方式 2 は全てのリンク鍵を知る基地局がリンク鍵を秘密情報として分散情報を作るため，CH とノードが必ず鍵共有を行うことが出来る．

次に，Kerberos をクラスタツリー型に適用した場合と比較を行うと，攻撃者が子ノードを盗難した場合，他のノード-CH 間のセッション鍵は漏えいしないことは同じだが，従来方式では，攻撃者に CH を盗難された場合 CH はクラスタ内の全てのセッション鍵を持っているため，クラスタ内の全てのセッション鍵が漏えいするという欠点がある．

一方, 提案方式 2 では Shamir の秘密分散法を用いることで分散情報のみを CH に持たせている．そのため情報量的安全性を持ち，もし CH を盗難された場合でも暗号通信用のリンク鍵が漏洩することはない．以上より、提案方式 2 は最初に示した(1)の特徴を実現する鍵共有方式となる．

5. 提案方式３

5.1 非対称秘密分散法

非対称秘密分散法[9]とは高橋らによって提案された新しい秘密分散法である．この方式では，特定のサーバの持つ分散情報の個数自体を削減することで，システム全体で持つデータ量の削減を実現している．この方式を用いることで，削減を行ったサーバの持つデータ量を鍵情報のみとすることができる．この方式を LEACH へ適用し鍵共有を考えると次のようになる．

5.2 LEACH への適用

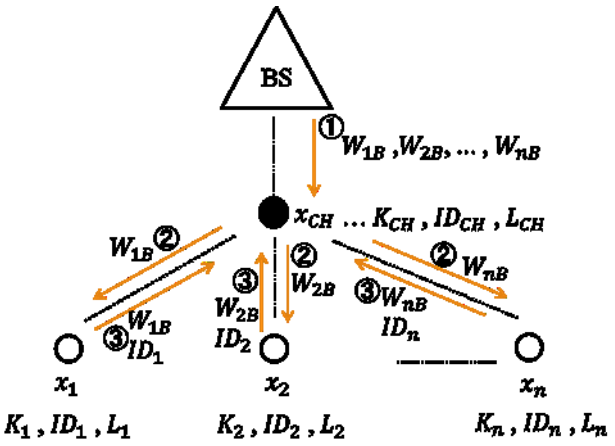

図 3.提案方式 3 の鍵共有方式

図 2 に CH(親ノード)●，子ノード○，基地局△をモデルとして，提案方式 3 の鍵共有方法について示す．提案方式 1 と同様に前提として各ノードに予め固有鍵(K_{CH}, K_1 , K_2 , …, K_n,)， ノード ID(ID_{CH}, ID_1, ID_2 , ID_3, … , ID_n,)， リンク鍵(L_{CH}, L_1, L_2, L_n)を持たせておく．これからノードのリンク鍵を秘密情報とし，以下の鍵共有を行う．

まずノード ID を BS へ知らせる．そこから基地局は各ノードのリンク鍵(L_{CH}, L_1, L_2, L_n)をそれぞれ秘密情報とするのだが，片方の分散情報$W_{1A}, W_{2A}, \dots, W_{nA}$をそれぞれノード ID: ID_1, ID_2 , ID_3, … , ID_n を CH の固有鍵 K_{CH} で暗号化したものに定める．その後に非対称型の秘密分散法を用いて，もう一方の分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$を生成する．その後の手順は以下のようになる．

① 各ノードの分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$ を CH へ送信する．

② CH は送られてきた分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$を対応する各ノードへ送信する．このとき CH は分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$を保持しない．

③ 各ノードは送られてきた分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$と自身のノード ID($ID_{CH}$, ID_2 , ID_3, … , ID_n,)を鍵共有する際に CH へ送信する．その後，CH は送られてきたノード ID を自信の持つ固有鍵 K_{CH} で暗号化し生成した分散情報$W_{1A}, W_{2A}, \dots, W_{nA}$と，送られてきたもう一つの分散情報$W_{1B}, W_{2B}, \dots, W_{nB}$を用いてリンク鍵 L_{CH}, L_1 , L_2 , L_n を復元する．

提案方式 3 を用いた場合でも，CH は暗号通信用のリンク鍵を保持していないため，もし CH が盗難された場合でもリンク鍵が漏洩することはない．さらにこの方式では，CH は各ノードに対応した分散情報を持つ必要がなくなるため CH の持つ鍵数を削減出来る．しかし，提案方式 3 では一方の分散情報をそれぞれノードの ID を CH の固有鍵 K_{CH} で暗号化したものに定めているために，安全性を提案方式 1 と比較した場合，情報量的安全性から計算量的安全性に落ちる．

5.3 評価・考察

続いて，提案方式 3 を従来方式と比較した場合でも，提案方式 1 と同様に暗号通信のセキュリティを考慮していて，かつ近隣の CH とノードが必ず鍵共有を行うことが出来る．また，CH が盗難された場合でも暗号通信用の鍵は漏洩しない．

一方，提案方式 2 と比較した場合は利点と欠点の両方が存在する．利点としては，CH の持つ鍵数を削減出来る点が挙げられる．これは高橋方式を用いて前述の分散情報を各ノード ID を CH の固有鍵で暗号化したものに定めているため，CH は固有鍵を持つだけで分散情報を生成出来るためである．欠点としては，前述のとおり片方の分散情報を各ノード ID を CH の固有鍵で暗号化したものに定めているため，提案方式 2 と比較した場合，安全性は情報量的安全性からその暗号化方式の安全性となる．

一般に，現在実用的に用いられる暗号化方式の安全性は計算量的安全性であるため，安全性は情報量的安全性から計算量的安全性に落ちる．以上より、提案方式 3 は最初に示した(2)の特徴を実現する鍵共有方式となる．

6. まとめ

クラスタツリー型のセンサネットワークにセキュリティに適した新しい鍵共有方式を提案した．本論文では 2 つの提案方式を挙げたが，一つ目の提案方式では，既存研究と比較した場合に CH を盗難された場合でも，暗号通信用の鍵に対して何の情報も漏洩しない利点がある．これは(2,2)の秘密分散法を用い，CH に一方の分散情報だけを持たせることで情報量的安全性を実現出来たためである．

二つ目の提案方式では，CH の持つ鍵の数を二つに削減出来た．この方式では秘密分散を用い，かつ一方の分散情報を CH の固有鍵でノードの ID を暗号化したものと定めることで，CH は固有鍵を持つだけで暗号通信用の鍵をノードと共有することが可能になった．また，この方式でも CH が盗難された場合でも鍵情報は漏洩せず，安全性は情報量的安全性から落ちるが，計算量的安全性を持つことが出来た．

謝辞　本研究を行うにあたって，ご指導を受け賜りました姜玄浩助教授に心から感謝致します．また，研究を行う際にご助力くださった東京理科大学岩村研究室の皆様に心から感謝致します．

参考文献

1) Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-Efficient Communication Protocol for Wireless Microsensor Networks. Proceedings of the 33rd Hawaii International Conference on System Sciences, January 4-7, (2000)
2) Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, Vol.1, No. 4, October (2002)
3) Oliveira, L.B., Ferreira, A., Vilaça, M.A., Wong, H.C., Bern, M., Dahab, R., Loureiro, A.A.: SecLEACH—On the Security of Clustered Sensor Networks. Signal Processing. Vol.87, No.12, pp. 2882-2895, (2007)
4) T. Qiang, W. Bingwen and W.COM Zhicheng “MS-Leach:A Routing Protocol Combining Multi-hop Transmissions and Single-hop Transmissions” Pacific-Asia Conference on Circuits, Communications and Systems, 2009, pp. 107-110,.
5) Chan H., Perrig A., Song D., : Random Key Predistribution Schemes for Sensor Networks. Proceedings of the 2003 IEEE Symposium on Security and Privacy, (2003)
6) Neuman B.C., Ts'o T.: Kerberos: an authentication service for computer networks. Communications Magazine, IEEE, Volume:32, Issue:9, pp. 33-38, (1994)
7) Sencun Z., Sanjeev S., Sushil J.: LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. ACM Transactions on Sensor Networks (TOSN), Volume 2, Issue 4, pp. 500-528, November, (2006)
8) A. Shamir. : How to share a secret, Communications of the ACM, pp.612-613 (1979)
9) 高橋慧 小林史郎 岩村惠市:『クラウドコンピューティングに適した計算量的安全性を持つ秘密分散法』　情報処理学会論文誌, Vol.53, No.10, 1-9 (Oct. 2012)