# ワイヤレスセンサネットワークにおける効率的なグループ鍵配送プロトコルの評価

三吉 雄大 †　　双紙 正和 †

† 広島市立大学　大学院情報科学研究科
731-3194　広島市安佐南区大塚東 3 丁目 4 番 1 号
miyoshi@sos.info.hiroshima-cu.ac.jp,soshi@hiroshima-cu.ac.jp

**あらまし** ワイヤレスセンサネットワーク（以後 WSNs）とは，ある種のセンサ（温度センサ，光センサ等）と無線通信機能を持つ安価な機器（以後ノード）を使って周囲の情報収集を行うためのワイヤレスネットワークである．ほとんどの場合，ノードはバッテリ駆動であり，リソースが限られている．そのため，複雑な暗号プロトコルの使用が制限されてしまう．この問題に対し，Eschenauer 等が WSNs 向けに鍵を事前に分配するプロトコル（以後 EG プロトコル）を提案した．そこで本論文では，EG プロトコルを前提として，ノードのエネルギー消費量を極力抑えながら効率的にグループ鍵を配送する手法の提案と評価を行う．

# Evaluation of Efficient Group Key Sharing Protocol for Wireless Sensor Network

Yuudai Miyoshi†　　Masakazu Soshi†

†Graduate School of Information Sciences, Hiroshima City University
3-4-1 Ohtuka-higashi,Asaminami-ku,Hiroshima-si,Hiroshima-ken 731-3194 JAPAN
miyoshi@sos.info.hiroshima-cu.ac.jp,soshi@hiroshima-cu.ac.jp

**Abstract** This paper propose and evaluate an efficient group key sharing protocol for wireless sensor networks, which is based on the protocol proposed by Eschenauer and Gligor.

## 1　はじめに

ワイヤレスセンサネットワーク（Wireless Sensor Networks，以後 WSNs）とは，ある種のセンサ（温度センサ，光センサ等）と，無線通信機能を搭載した安価な機器（以後ノード）を広範囲に多数配置して周囲の情報を収集する，無線ネットワークの一種である．一般的なネットワークと同様，WSNs においてもセキュリティは重要な課題の一つとなっている．しかし，ノードは安価で低性能なものを使用するのが一般的であり，記憶容量，計算能力が乏しく，バッテリ駆動であるため消費電力を考慮する必要がある．そのため，計算量の多い暗号プロトコル，特に公開鍵暗号方式での暗号通信を行うことは困難である．この問題に対して，Eschenauer と D.Gligor によって，鍵を事前に分配しておく手法（以後 EG プロトコル）が提案された [4]．この手法は，あらかじめ鍵を大量に生成しておき，各ノードに鍵の部分集合を割り当てることにより，ノード同士が確率的に秘密鍵を共有できるようにしたものである．

WSNs は無線ネットワークであり，基地局とノード，ノードとノード同士の通信はブロードキ

ャストで行われる一つのノードから多数のノードへの同時通信が可能であり，そのため，一対一の通信を $N$ 回繰り返すよりも，一対 $N$ 通信（以後グループ通信）を一回行う方が効率的である．そして，セキュアに一対 $N$ 通信を行うために，$N$ 個のノードでグループを作り，そのグループ内のノード（以後グループノード）で共通のグループ鍵を共有することが望ましい．安全性を考慮すると，グループ鍵を攻撃者に取得されないようにグループ鍵の共有はノード毎に一対一通信を $N$ 回行うことが望ましいが，効率的ではない．そのために，一回のブロードキャストでグループノードにグループ鍵を効率的に配送する手法が研究されている．

本論文では，*EG* プロトコルを前提としてグループ鍵を効率的に配送するプロトコルを提案し，考察を行う．*EG* プロトコルを前提としたグループ鍵配送プロトコルでは，一対一通信を $N$ 回行うよりも少ない通信量でグループ鍵を共有することができ，ノードの電力消費を抑えることが可能である．

本論文は以下のように構成される．2 章で関連研究の紹介を行う．3 章で提案手法の紹介を行う．4 章で提案手法を評価するための実験と評価を行う．5 章でまとめとなる．

## 2 関連研究

一般的なネットワークにおける暗号通信は，公開鍵暗号方式が用いられている．公開鍵暗号方式では，ある種の数学的問題の困難性に基づいて暗号化および復号化を行うことで，暗号化する鍵と復号する鍵を異なる物にすることが出来る [3]. そのため，暗号化する鍵を盗聴されても安全性が損なわれることはない．しかし，暗号化，および復号にかかる計算量が多くなってしまうという欠点があり，WSNs で利用するとノードに負荷がかかってしまい，適切ではない．そのため，WSNs では共通鍵暗号方式を利用するのが一般的である．共通鍵暗号方式では，暗号化と復号に同じ鍵を利用するものである．これにより，暗号化，復号にかかる計算量は抑えることが出来る．共通鍵の共有の際に鍵を攻撃者に盗聴されると情報の復号が容易であるという欠点を持つ．WSNs で共通鍵暗号方式を利用する手法として，例えば全てのノードで同じ鍵を利用する手法が考えられる．これによって，容易に，通信を行っている情報を盗聴されても一目では分からない形にすることができる．しかし，何らかの形で攻撃者が鍵を得てしまった場合，全ての情報を攻撃者が復号出来るという大きな問題点が存在する．そのため，通信路毎にユニークな鍵を利用することで，攻撃者が一つ鍵を得ても，ネットワーク全体への影響は最小限に抑えることが出来る．しかし，それを実現するためにはノードの記憶容量が問題となる．ノードの配置はランダムで行われる場合が多い．ノードが近傍のノードと確実に通信を行うためには，全てのノードが持っている鍵を所持しておく必要がある．単純に考えると，ネットワーク上に $N$ 個のノードが存在している場合，ノード一つに $N-1$ 個の鍵を持たせる必要がある．ノードの数が増えた場合，ノードが持つべき鍵の量も多くなる．WSNs においては，数百から数十万のノードでの利用が想定されており，各ノードに必要な鍵を全て保持させることは現実的ではない．

そこで，Eschenauer と D.Gligor が WSNs 向けの鍵共有プロトコルを提案した [4]．このプロトコルは，多くの WSNs における鍵共有プロトコルの基礎となっている．EG プロトコルは，鍵分配段階，通信路設立段階に分かれる．まず，鍵分配段階の説明を行う．鍵分配段階は，ノードを目的としている地域に配置する前に行われる．無作為かつ大量に生成した鍵の集合（以後鍵プール）を作成する．鍵プールから，無作為に一定サイズの部分集合（以後鍵リング）をノードの数だけ作成し，それぞれを各ノードのメモリに保存していく．次に通信路設立段階の説明を行う．通信路設立段階は，ノードを地域に配置してから行われる．各ノードは，自分と 1hop で通信が可能な範囲に他のノードが存在するか確認する．そして，ノードが存在していた場合，その隣接するノードと鍵リングを比較し，同じ鍵を保存していた場合，同じ鍵の中から一つを選んで暗号通信を開始する．これが，EG プロト

コルである．EG プロトコルの利点は二つ存在する．一つ目は，通信路毎では共通鍵暗号方式で暗号通信を行っているのでノード単位での計算量を抑えることが出来るという点である．二つ目は，全ての通信路で使用する鍵をノードが保存しておく必要が無く，ノードのメモリを節約できる点である．しかし EG プロトコルには大きな問題点が存在する．ノードを物理的に発見，解析するノード捕縛攻撃に弱いという点である．ノードを捕縛され，そのノードの鍵リングを知られてしまった場合，その鍵を利用している通信路での暗号通信が解読されてしまう．少数のノードの捕縛であれば影響は少ないが，大量に捕縛されてしまった場合，ネットワークで利用している鍵を全て，すなわち鍵プールが知られてしまい，ネットワーク全体が盗聴可能になる危険が存在している．この問題に対抗する手段が研究されている．例えば Chan 等は，1 つの経路に 1 個以上の鍵を合成して使う手法を提案した [2]．また，Liu 等は EG プロトコルに Blundo の方式 [1] を適用して，ノード捕縛攻撃に対して耐性を持たせる手法を提案した [5]．

WSNs では，通信回数を少なくするためにグループ鍵をグループノードで共有してグループ通信を行うことが多い．WSNs においては通信はブロードキャストになるため，セキュアな通信を行うためにもグループ鍵をグループノードで共有するのが望ましい．グループ鍵を共有することで，グループ内であれば全ての通信をブロードキャストで行えるという利点がある．しかし，グループ鍵をセキュアに共有するためには，まず一対一で基地局と通信を行う必要がある．そこで，グループ鍵を一度の通信でグループノードで共有する手法が研究されている．例えば Zheng 等が，中国人の常用定理を用いたグループ鍵共有方式を提案している．これによって，一つの値を送るだけで他のノードの秘密鍵を知らなくても複数のノードにグループ鍵を配ることが出来る．しかし，中国人の剰余定理の性質により，グループノードの数が多いほど計算量が増大してしまう欠点を持っている．

## 3 提案手法

EG プロトコルによって複数の共通鍵の分配が行われた後という限定的な環境下でグループ鍵を配送する手法を提案する．なお，基地局は各ノードの鍵リングを全て把握しているものとする．

まず，$p$ を暗号に使うことの出来る大きな素数とし，WSNs 上には $N$ 個のノードが存在しているとする．そして，基地局は $m$ 個のノードをグループとしてグループ鍵を配送するものとする．基地局はグループ鍵 $\alpha$ と乱数 $r$ を生成する $(\alpha, r \in Z_p^*)$．次に，$m$ 個のグループノードで共通する，出来るだけ少ない鍵の二つ組みの集合 $(k_{11}, k_{12})$,$(k_{21}, k_{22})$……$(k_{i1}, k_{i2})$(i=1,2,……,l) を探す．そして基地局は，探索した鍵の組の集合を元に，以下のような多項式

$$f(x) = (x - h(r, k_{11}, k_{12}))(x - h(r, k_{21}, k_{22}))\cdots (x - h(r, k_{i1}, k_{i2})) + \alpha$$

を生成する．なお，$h(a, b, c)$ は $a, b, c$ を変数とする暗号学的ハッシュ関数である．

乱数 $r$ は，乱数要素を交えることで，複数回グループ鍵を配送する際の安全性を高める狙いがある．鍵を二つ組にして多項式で利用している理由は，各項において一つずつ鍵を使用する手法において，グループ鍵が漏洩する確率が高いという欠点が存在しているからである [6]．基地局が多項式を生成する際に選んだ鍵を一つでもグループノードではないノードが持っていた場合，多項式を容易に解くことができ，危険である．そのため，鍵を二つ組にして多項式を生成することで鍵の組を非グループノードが持つ確率を下げる狙いがある．

多項式 $f(x)$ を変形し，以下のような多項式 $g(x)$ とする．

$$g(x) = x^m + \Sigma_{i=0}^{m-1} a_i x^i$$

次に基地局は乱数 $r$，$a_1, a_2, ..., a_{m-1}$,$E_\alpha(M)$ をブロードキャストする．なお，$E_\alpha(M)$ はあるメッセージ $M$ をグループ鍵 $\alpha$ で暗号化したものであり，メッセージ $M$ は公開されており全てのノードが知り得る．情報を受信したノード

は，まず乱数 $r$，$a_1, a_2, ..., a_{m-1}$ を使って $g(x)$ を構築する．そして，各々が持つ共通鍵で作った鍵の二つ組と受信した乱数 $r$ を使って多項式 g(x) を解く．そして得た値を使って $E_\alpha(M)$ を復号し，結果をメッセージ $M$ と比較する．ノードが鍵の二つ組を正しく選んでいた場合の値で復号すると，メッセージ $M$ を得ることが出来る．つまり，算出した値がグループ鍵と等しいため．その値をグループ鍵として保存する．以上が提案手法となる．

# 4 実験

提案したグループ鍵配送プロトコルの評価を行うために実験を行った．

## 4.1 実験目的

提案した手法は *EG* プロトコルを前提としている．しかし EG プロトコルは乱数要素が多く，定量的な評価が難しい．そこで，シミュレータを使用して提案プロトコルの評価を行っていく．

## 4.2 実験環境

実験に使用した計算機の環境を表 1 に，シミュレーションのパラメータを表 2 に記す．

| | |
|---|---|
| コンピュータ型番 | hp xw8400 workstation |
| CPU | Intel(R) Xeon(TM) CPU 3.60GHz 2 個 |
| memory | 3GB |
| OS | Microsoft Windows XP Professional x64 Edition Version 2003 Service Pack 1 |
| 開発環境 | gcc 4.0.1 |
| プログラミング言語 | C++ |

表 1: 実験環境

| | |
|---|---|
| Number Of Node | シミュレーション環境に存在するノードの総数 |
| Key Pool Size | EG プロトコルにおいて作成する鍵プールのサイズ |
| Key Ring Size | EG プロトコルにおいてノードに保存する鍵リングのサイズ |
| Repeat | 試行回数 |
| Number Of Target Nodes | グループ鍵を配送するグループノードの数 |

表 2: シミュレーションパラメータ

## 4.3 通信量の評価

基地局からノードへ送られる多項式は，各項の係数だけを送る．そのため，多項式の次数は送る係数の個数となり，通信量に直結する．通信量の評価を行うために，多項式の次数がパラメータによってどのように変動するかを調査する実験を行った．

### 4.3.1 実験手法

なるべく多くのグループノードで共通する鍵の二つ組の集合を探索する手法について，以下のような二つの手法をシミュレータで実装し，次数の変動を調査した．なお，この実験で使用したシミュレーションパラメータを表 3 に記した．

一つ目の選択手法として，ランダムに鍵を選択するものが挙げられる．以下のような手順で鍵を選択した．

1. ノードを Number Of Nodes 個生成し，鍵を Key Pool Size 個生成して鍵プールとする．
2. 鍵プールから Key Ring Size 個をランダムに選出し，鍵リングとして各ノードに分配する．
3. ノード全体から Number Of Target Nodes 個のノードを選出し，グループノードの D

リストを作成する．

4. グループノードの一つからランダムに鍵を二つ選出し，鍵 A，鍵 B とする．
5. グループノード全体を調査し，鍵 A，鍵 B を両方持っているノードをグループノードの ID リストから削除していく．
6. 手順 4, 手順 5 を繰り返し，グループノードの ID リストが空になった時の繰り返し回数を共通する鍵の二つ組の数，つまり次数と定める．
7. 手順 4〜手順 6 を Repeat 回繰り返して次数の平均を求める．

二つ目の選択手法として，グループノード全てが持つ鍵で作ることが出来る鍵の二つ組を総当たりで調査し，なるべく複数のノードが持っている鍵の二つ組を選択する手法が挙げられる．以下のような手順で鍵を選択した．

1. ノードを Number Of Nodes 個生成し，鍵を Key Pool Size 個生成して鍵プールとする．
2. 鍵プールから Key Ring Size 個をランダムに選出し，鍵リングとして各ノードに分配する．
3. ノード全体から Number Of Target Nodes 個のノードを選出し，グループノードの ID リストを作成する．
4. グループノードが持つ鍵で作ることが出来る鍵の二つ組を全て調査し，鍵の組で鍵リストを作成し，組の数をカウントしていく．
5. 鍵リストのうち，一番多くのノードが持っている鍵をそれぞれ鍵 A，鍵 B とする．
6. グループノード全体を調査し，鍵 A，鍵 B を両方持っているノードをグループノードの ID リストから削除し，更に鍵 A，鍵 B の組を鍵リストから削除する．
7. 手順 5, 手順 6 を繰り返し，グループノードの ID リストが空になった時の繰り返し回数を共通する鍵の二つ組の数，つまり次数と定める．
8. 手順 5〜手順 7 を Repeat 回繰り返して次数の平均を求める．

| | |
|---|---|
| Number Of Node | 100 |
| Key Pool Size | 100 |
| Key Ring Size | 5〜70 |
| Repeat | 100 |
| Number Of TargetNodes | 10 |

表 3: 実験パラメータ

### 4.3.2 実験結果

シミュレーションを行った結果を，図 1 に示した．横軸は鍵リングのサイズの変動，縦軸が次数の変化を表し，凡例は『random』がランダムに鍵を選択した場合の多項式の次数を表し，『ALL』が総当たりで調査した場合の多項式の次数を表している．

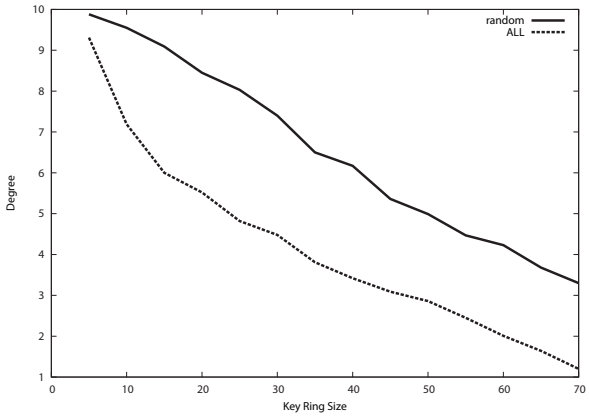


図 1: 提案手法における次数の変化

## 4.4 考察

図 1 を見ると，ランダム，総当たり，共に，鍵リングのサイズが大きくなると次数が下がっているのが分かる．鍵の組を共通で持つノードの比率が上がっているのである．これは直感的にも明らかである．上述の通り，多項式の次数は

提案プロトコルにおいては通信量に直結する．鍵プールのサイズは固定であるから，鍵プールのサイズに占める鍵リングのサイズの比率が大きくなれば次数は下がり，結果として通信量は下がる．

鍵をランダムに選択する場合のグラフは，意図的に鍵の組が重複するように選んだ際の次数の上限に近似していると言える．

また，鍵を総当たりで調査する場合のグラフは，意図的に鍵の組が重複するように選んだ際の次数の下限に近似していると言える．なお，総当たりで調査した場合の次数は，集合被覆問題の存在によって必ずしも最適解であるとは言えない．

WSNs が大規模になると，総当たりで調査すると計算量が膨大になる．そのため，意図的に鍵の組が重複するように，しかしなるべく計算量が少なくなるような手法が必要である．

## 5　まとめ

EG プロトコルによって共通鍵の共有が行われている WSNs という限定された環境下に特化したグループ鍵配送プロトコルの提案を行い，その評価実験を行った．今後の課題として，以下の二つを挙げる．一つ目に，なるべく次数が小さくなるような鍵の組の検索手法の発見が挙げられる．二つ目が，多項式を解く際にノードが行う計算の簡略化である．各ノードからなるべく多くのノードで共通する鍵を一つずつ取ってくる手法 [6] においてはノードがグループ鍵を算出する計算量は高々線形時間であるが，提案手法においては多項式時間まで増大してしまう．そのため，ノードが行う計算を簡略化する手法が必要である．

## 謝辞

本研究は科学研究費補助金 (21240001,20300003) の助成を受けたものである．

## 参考文献

[1] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly secure key distribution for dynamic conferences. *Information and Computation*, Vol. 146, No. 1, pp. 1–23, 1998.

[2] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, p. 197, Washington, DC, USA, 2003. IEEE Computer Society.

[3] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on information Theory*, Vol. 22, No. 6, pp. 644–654, 1976.

[4] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 41–47, 2002.

[5] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 8, No. 1, pp. 41–77, 2005.

[6] 双紙正和三吉雄大. ワイヤレスセンサネットワークにおける効率的なグループ鍵配送プロトコル (情報通信システムセキュリティ). 電子情報通信学会技術研究報告, Vol. 110, No. 266, pp. 7–10, 2010-11-05.