2007－CSEC－39 (7)
2007／12／14

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

大網優太 斎藤誠 岩村惠市
東京理科大学
〒102-0073 東京都千代田区九段北 1-14-1

あらまし

センサネットワークに対する、新しい鍵事前格納方式を提案する。センサネットワークは、センサノードにより自立的に構成されたアドホックネットワークの一種である。センサノードはごく限られた電源容量と演算性能しか持たないため、Diffie-Hellman 鍵共有プロトコルや公開鍵暗号技術の利用等、比較的大きな計算量が必要となる処理を行うことは好ましくない。そのため、少ない計算量で暗号鍵の共有を可能にする方法として、鍵事前格納方式が研究されている。本研究では、KPS の可用性およびランダム鍵事前格納方式の安全性を利用した融合方式を提案し、同方式の可用性および耐盗難性を評価する。

キーワード センサネットワーク、アドホックネットワーク、鍵共有、鍵事前格納方式

A Key Pre-distribution Scheme for Wireless Sensor Networks

Yuta Ooami Makoto Saito Keiichi Iwamura
Tokyo University of Science
1-14-1 Kudan-Kita, Chiyoda-Ku, Tokyo 102-0073, Japan

Abstract

We suggest a new key prior storage method for the sensor network. The sensor network is a kind of an ad hoc network constituted autonomously by a sensor node. Because the sensor node has only extremely limited power supply capacity and operation performance, it is unfavorable that comparatively big computational complexity such as a Diffie-Hellman or public key based scheme. Therefore, as a method to share the encrypting key in little computational complexity, a key prior storage method is studied. In this study, we propose a new scheme which united random key pre-distribution scheme [6] and KPS [8]. Then this scheme gets the safety of random key pre-distribution scheme and the availability of KPS.

1 はじめに

共通鍵暗号[1]を用いて、センサネットワークのセンサノード間で暗号通信を行うために、鍵事前格納方式[4,5,6,7]が研究されている。センサノードは外部から電源が供給されず、ノードに内蔵された電池を用いて各種の処理を行うため、センサノードの演算能力や記憶容量は低く抑えられている場合が多い。また、センサノードは、物理的に保護されない場所に設置されることが多く、常に盗難の危険性に晒されていると考える必要があるが、実装コスト等の関係でノードそのものに耐タンパ性を期待することは出来ない。このような2台のセンサノードが通信を行う際に、従来は可用性と耐盗難性の二つの性能指標について考慮することが一般的である。可用性とは、ノードの接続トポロジを予見できないセンサネットワークにおいて隣接するノードと、高い確率で鍵の合意に成功する性質をいう。また、耐盗難性とはセンサネットワークの安全性を確保するために、悪意を持った攻撃者が少数のセンサノードを入手し、それらのノードに格納された鍵を知ったと

しても、盗難にあっていないノード間通信の安全性が損なわれない性質をいう。

鍵事前格納方式では、工場出荷時に、センサノードへあらかじめ複数の鍵を格納しておく。従来のセンサネットワークに対する鍵共有方式としてはランダム鍵事前格納方式[4-7]が主に用いられている。この方式はいくつか研究が行われているが、いまだ完全な可用性が実現されていない。一方、他の鍵共有方式としてKPS(Key Pre-distribution Scheme)と呼ばれる方式[8]等が知られている。KPSは小さなリソースで実現でき、また必ず鍵共有ができるが、1ノードの盗難によって取られる情報量が多く、盗難耐性が弱い。

本研究では、ランダム鍵事前格納方式に一部KPSを取り入れる方式を提案する。これにより、KPSによる確実な鍵共有（可用性）、ランダム鍵事前格納方式による高い耐盗難性を両立させる鍵共有方式を実現する。以降、第2章では既存研究を説明し、第3章では提案方式の説明、第4章では提案方式の評価法を検討し、第5章では既存研究との比較を行う。

2 既存研究

2.1 センサネットワークにおける鍵共有方式

センサネットワークにおける鍵共有には、様々な方式があるが、本論文では基地局の存在を仮定せず、ノード間だけで暗号化通信を行う方式について考え、ノード間だけで直接通信を行う場合にも適用可能な暗号化手法について議論する。

最も基本的な鍵共有方式の1つとして、ノード間通信の暗号化に1つの鍵（global key）だけを利用する方式が考えられる。全てのノードにこのglobalkeyをあらかじめ格納しておくことで、任意のノード間で通信が可能となる。しかし、この方式では何らかの理由で1つのノードから鍵が漏洩してしまった場合、ネットワーク全体の安全性がすべて失われてしまうので、実用的な方式とは言い難い。そのため上記の問題に対し、Eschenauerらによりランダム鍵事前格納方式が提案されている[4]。

2.2 鍵事前格納方式

[4]の提案法は、事前に各ノードに鍵を割り当てる鍵事前格納法とノード間で通信に用いる暗号鍵を生成するリンク鍵確立法からなる。ランダム鍵格納方式は、リンク毎に異なる鍵を割り当てる方式を近似的に実現する方式であると考えることができる。鍵管理者は、大量の鍵を要素として含む鍵集合S（以下、**鍵プール**と呼ぶ）をあらかじめ定めておき、各ノードには、Sから無作為に選ばれた$m(\geq 1)$個の鍵を工場出荷時に事前格納する。Sの要素を**要素鍵**と呼び、ノードnに格納された要素鍵の集合を$K(n)$と書くことにする。また、要素鍵には識別子が付与されているものと仮定する。工場出荷後、二つのノードが暗号化通信を行う際には、リンク鍵確立法により、暗号化に用いる暗号鍵（これを本稿では**リンク鍵**と呼ぶ）の共有を行う。2台のノードをn_1, n_2とするとき、n_1, n_2はそれぞれ、自分の持っている鍵の識別子を相手に知らせ、何らかのプロトコルを用いて、$K(n_1) \cap K(n_2)$の中の鍵を1つ特定し、これをリンク鍵とする。しかし、攻撃者はリンク鍵として使われている1つの要素鍵を取得できれば、暗号化された通信の盗聴に成功してしまうため、耐盗難性は高いとはいえない。

[4]の改良法として、q－複合鍵方式が提案されている[5]。この方式は、鍵事前格納法については[4]と同じであるが、リンク鍵確立法を改良したものとなっている。[4]ではノード間で1つでも共有する要素鍵があればリンク鍵を確立できたのに対し、この方式では、共有する要素鍵が少なくともq個以上なければリンク鍵を確立できない点が異なっている。しかし、リンク鍵の共有に必要となる条件が厳しくなっているため、リンク鍵の確立に成功する確率が低くなりがちである。

[4][5]を基にさらに可用性と耐盗難性を高めた提案方式として[6]がある。[6]は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である。比較的小さな鍵プールを複数準備し、各鍵プールからランダムに1つずつ選んだ要素鍵をノードに事前格納する。2ノード間のリンク鍵は両ノードが共有する要素鍵全てを用いて定義する。これにより、攻撃者はリンク鍵を構成する全ての要素鍵を知ることが出来ない限り、リンク鍵を知ることが出来ない。しかし、2台のノード間でリンク鍵が共有されるとは限らないため、可用性の面において難が生じる可能性がある。

[6]とは別のアプローチの方式で[7]がある。この方式は[6]の方式より可用性に優れ、耐盗難性に劣る方式であるが、これも確実な通信は実現されていない。

2.3 KPS

ランダム鍵事前格納方式とは別のアプローチとして KPS が提案されている[8]。KPS は ID ベースの鍵共有方式の一つである。ID ベース鍵共有方式には通信を必要とする方式と必要としない方式があり、KPS は通信を必要としない方式である。

KPS は、図 1 を参照することで必ず鍵共有が成立する方式である。K_{xy} はノード x とノード y の共有鍵を表す。しかし、攻撃者にノード I が盗まれることによってノード I に関わる全ての通信内容が漏れてしまうことを表すので耐盗難性に問題がある。

ID	1	2	…	i	…	j	…	n
1	K_{11}	K_{12}	…	K_{1i}	…	K_{1j}	…	K_{1n}
2	K_{21}	K_{22}	…	K_{2i}	…	K_{2j}	…	K_{2n}
…	…	…	…	…	…	…	…	…
i	K_{i1}	K_{i2}	…	K_{ii}	…	K_{ij}	…	K_{in}
…	…	…	…	…	…	…	…	…
j	K_{j1}	K_{j2}	…	K_{ji}	…	K_{jj}	…	K_{jn}
…	…	…	…	…	…	…	…	…
n	K_{n1}	K_{n2}	…	K_{ni}	…	K_{nj}	…	K_{nn}

図 1　KPS の鍵生成関数参照表

3　提案方式

提案方式では、[6]のランダム鍵事前格納方式に一部 KPS[8]を取り入れ、ランダム鍵事前格納方式で用いていた n 個の秘密情報の内 l 個を KPS で用いる。2 ノード間のリンク鍵は両ノードが共有する要素鍵全てを用いて定義する。すなわち、KPS で共有できる鍵に加えて、ランダム鍵事前格納方式で共有できる鍵全てを用いて、リンク鍵を生成する。これにより、攻撃者はリンク鍵を構成する全ての要素鍵を知ることが出来ない限り、リンク鍵を知ることが出来ない。また、ノード間の鍵共有が確実であり、可用性との両立が実現できる。[7]の方式を用いず、[6]の方式を選んだのは、KPS によって通信の確実性が保証されるのであれば全体の安全性が高い方式を融合した方が有効だからである。

S を鍵の全体集合とし、S_{ran} をランダム鍵事前格納方式部、S_{kps} を KPS 部とすると、

$$S = S_{ran} + S_{kps}$$

と表すことができる。

ランダム鍵事前格納方式部は、[6]に基づき、小さな鍵プールを複数準備し、各鍵プールからランダムに 1 つずつ選んだ要素鍵を事前格納する。ランダム鍵事前格納方式部で使える秘密情報量は $n-l$ であるため、鍵プール数は $n-l$ 個である。ここでリンク鍵を共有したい 2 台のノードを n_1, n_2 とし、$K_{ran}(n_i)$ はノード i のランダム鍵事前格納方式部の要素鍵とする。また、$K_{ran}(n_1) \cap K_{ran}(n_2) = \{k_1 \| k_2 \| \ldots \| k_i\}$ とする。$K_{ran}(n_1) \cap K_{ran}(n_2) = 0$ のとき、n_1 と n_2 はリンク鍵の共有に失敗するため、最低限の暗号通信を KPS 部に委ねる。

KPS 部は、n 個のノードがあったならば n 個の秘密情報が必要な方式であるが、今回利用出来る秘密情報は、n 個のノードに対して $l(<n)$ 個の秘密情報しかない。したがって、KPS の鍵削減法を考える必要がある。これは $l \times l$ の対称マトリクス（図 2）を生成することによって実現する。

ID	1	2	…	i	…	l
1	K_{11}	K_{12}	…	K_{1i}	…	K_{1l}
2	K_{21}	K_{22}	…	K_{2i}	…	K_{2l}
…	…	…	…	…	…	…
i	K_{i1}	K_{i2}	…	K_{ii}	…	K_{il}
…	…	…	…	…	…	…
l	K_{l1}	K_{l2}	…	K_{li}	…	K_{ll}

図 2　KPS の鍵削減法

KPS と同様、K_{xy} はノード x とノード y の共有鍵を表す。ID i を持つノード I には 1～l のプールの内、$i \bmod l$（0 の時は l とする）に該当するプールを配布する。$l(<n)$ であるために同じ鍵プールが配布される状況が想定される。これは耐盗難性において欠点となるが、その部分の安全性はランダム鍵事前格納方式部に依存する。KPS 部では共有される要素鍵は 1 つである。例外は同じ鍵プール i を与えられ

た場合で、保有する共通の鍵情報はK_{i1}～K_{il}のl個となる。しかし、盗難における耐性という点を考えると対角線上の鍵情報K_{ii}が、同じ鍵プールを持っている際にしか使われない固有の情報となるため、K_{i1}～K_{il}を共有している場合とK_{ii}についてのみ考える場合は同義であると考えられる。よって、ここで鍵を共有したい 2 台のノードをn_1, n_2とするとき$K_{kps}(n_1) \cap K_{kps}(n_2) = \{k'\}$となる。

最終的なリンク鍵はランダム鍵格納方式部と KPS 部の共有する要素鍵を複合して

$$h(k_1 \| k_2 \| \ldots \| k_i \| k')$$

で定義される。ここで、hは一方向ハッシュ関数であり、$x \| y$はxとyの連結を表す。攻撃者は$K(n_1) \cap K(n_2)$に属する全ての要素鍵を知らない限り、リンク鍵を知ることができない。

4 提案法の評価

4.1 可用性

ここでは、ランダムに選ばれた 2 台のノードが高い可用性を有することを示す。リンク鍵共有確率とは、ランダムに選んだ 2 台のノードn_1, n_2に対し、$K(n_1) \cap K(n_2) \neq 0$となる確率と定義する。$K(n_1) \cap K(n_2) \neq 0$ならば、$n_1$と$n_2$はリンク鍵の共有に成功するため、リンク鍵共有確率が大きいほど、方式の可用性は高いといえる。

ランダム鍵事前格納方式部のリンク鍵共有確率p_{ran}は$1-(1-1/(n-l))^{n-l}$である[6]。

KPS 部は、必ず共有する鍵があるために、リンク鍵共有確率p_{kps}は 1 となる。

よって、本提案方式はランダム鍵事前格納方式で鍵が共有できなくても KPS で必ず鍵共有できるため、全体のリンク鍵共有確率pは 1(100%)となる。

4.2 耐盗難性

攻撃者がセンサネットワーク内のc台のノードを盗難し、そのノードに格納された要素鍵を全て知ったとする。もし、$K(n_1) \cap K(n_2)$が盗難ノードの要素鍵集合の部分集合だとすると、攻撃者はノードn_1, n_2間のリンク鍵を知ることができる。ここでは、攻撃者がリンク鍵を知る確率について評価する。$n'_1, n'_2, \ldots, n'_c$を攻撃者が入手したc台のノードとする。$n_1, n_2 \notin \{n'_1, \ldots, n'_c\}$、$K(n_1) \cap K(n_2) \neq 0$に対し、

$$K(n_1) \cap K(n_2) \subset \bigcup_{i=1}^{c} K(n'_i)$$

となる確率を**リンク鍵危殆化確率**qと定義する。リンク鍵危殆化確率が小さいほど、方式の耐盗難性は高いといえる。リンク鍵はランダム鍵事前格納方式部と KPS 部で共有される全ての要素鍵を用いて作られるため、全体のリンク鍵を知るには、双方の要素鍵全てを知らなければならない。よって、全体のリンク鍵危殆化確率qは、ランダム鍵事前格納方式部のリンク鍵危殆化確率q_{ran}と KPS 部のリンク鍵危殆化確率q_{kps}の積で表される。

ランダム鍵事前格納方式部についてkを$K_{ran}(n_1) \cap K_{ran}(n_2)$に属する鍵とする。盗難された$c$台のノードに$k$が格納されていないとき、攻撃者は$k$を知ることはない。攻撃者が盗難した$c$台のノードから$k$を知る確率$p_c$は、$1-(1-1/(n-l))^c$である。$n_1, n_2$間のリンク鍵を計算するには、攻撃者は$K_{ran}(n_1) \cap K_{ran}(n_2)$に属する全ての鍵を見つける必要があり、$K_{ran}(n_1) \cap K_{ran}(n_2)$が$s$個の要素鍵を含んでいるとすれば、その確率は$p_c^s$である。$K_{ran}(n_1) \cap K_{ran}(n_2)$に属する鍵の数は二項分布に従うため、$K_{ran}(n_1) \cap K_{ran}(n_2)$が$s$個の要素鍵を含む確率$t_s$は

$$\binom{n-l}{s}\left(\frac{1}{n-l}\right)^s\left(1-\frac{1}{n-l}\right)^{n-l-s}$$ である。

以上より、c台のノードを盗難した攻撃者がリンク鍵を知る確率は、以下の式で与えられる。

$$e_c = \sum_{s=1}^{n-l} t_s p_c^s = \sum_{s=1}^{n-l}\binom{n-l}{s}\left(\frac{1}{n-l}\right)^s\left(1-\frac{1}{n-l}\right)^{n-l-s} p_c^s$$

$$= \left(1-\frac{1}{n-l}\left(1-\frac{1}{n-l}\right)^c\right)^{n-l} - \left(1-\frac{1}{n-l}\right)^{n-l}$$

リンク鍵危殆化確率は、$K_{ran}(n_1) \cap K_{ran}(n_2) \neq 0$のもとでの条件付き確率なので、

$$q_{ran} = \frac{e_c}{p_{ran}}$$
$$= \frac{1}{p_{ran}}\left(\left(1-\frac{1}{n-l}\left(1-\frac{1}{n-l}\right)^{c}\right)^{n-l} - \left(1-\frac{1}{n-l}\right)^{n-l}\right)$$

となる。ここで、p_{ran}はランダム鍵事前格納方式部におけるリンク鍵共有確率である。

次に KPS 部について考える。k'を$K_{kps}(n_1)\cap K_{kps}(n_2)$に属する鍵とする。盗難された$c$台のノードに$k'$が格納されていないとき、攻撃者は$k'$を知ることはない。攻撃者が盗難した$c$台のノードから$k'$を知る確率は、

$$q_{kps} = 1-\left(\frac{(l-1)^2}{l^2}\right)^{c}$$

となる。

5 既存研究との比較

本節では、文献[6]にて提案されているランダム鍵事前格納方式、文献[8]にて掲載されている KPS と提案法の性能を比較する。比較の前提を同じにするために、各々の方式で 1 ノードに配布する秘密情報量をn個とする。

5.1 可用性の比較

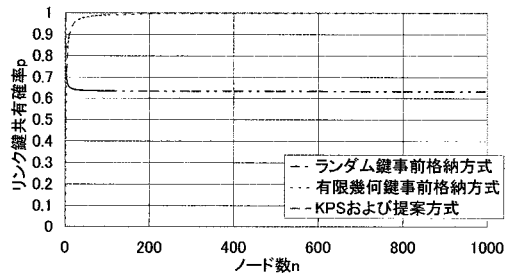

図3 ノード数ーリンク鍵共有確率

図 3 からもわかるようにある程度のノード数になった際ランダム鍵事前格納方式は、0.6321 付近に収束する。これは同じ条件下では 3 回に 2 回程度の共有しか出来ないことを表す。有限幾何方式は、ノード数 200 あたりから限りなく 1 に近い値をとる。

5.2 耐盗難性の比較(KPS 部＋ランダム部)

既存技術と提案方式($l = n/2, n/3, n/4, 1$を代表例とする)を$n = 100$のもと比較したものを図 4 に示す。この前提として$K_{ran}(n_1)\cap K_{ran}(n_2)\neq 0$、すなわちランダム鍵事前格納方式部の要素鍵でリンク鍵が共有できた場合を考え、$K_{ran}(n_1)\cap K_{ran}(n_2) = 0$、すなわちランダム鍵事前格納方式部の要素鍵でリンク鍵が共有できなかった場合については後の 5.3 で述べる。ランダム鍵事前格納方式部の要素鍵でリンク鍵が共有できた場合とは、従来のランダム鍵事前格納方式で可用性が実現できた場合を意味する。

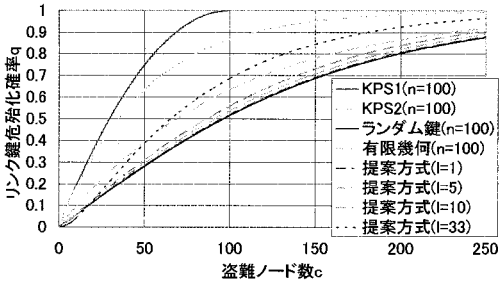

図4 盗難ノード数-リンク鍵危殆化確率

破線は既存技術を示し、実線は提案方式を表す。安全性は傾きが緩やかであるほど高い。

KPS1 は、1 対 1 対応の鍵共有方式であるため、各ノードに配布される秘密情報量nが 100 であれば全体のノード数も 100 である。よって盗難ノード数が 100 の時全体の秘密情報が漏洩するため、1 に収束している。

KPS2 は、同じ鍵プールが配布される可能性のある KPS であるため、秘密情報量nが 100 の時点ではまだ収束しない。また、ランダム性が出てくるため、全体として KPS1 より高い耐盗難性を持つ。

ランダム鍵事前格納方式は現在考えられている最も安全性の高い方式であるため、傾きは最も緩やかである。ただし、これはリンク鍵共有確率を犠牲にした安全性の高さである。

提案方式は、確実なリンク鍵共有が可能であるという前提のもと既存技術 KPS を常に上回る耐盗難性を持つ。次に、$l = 1$の時、提案方式の安全性はランダム鍵事前格納方式とほとんど変わらないことが認められる。また、$l = n/4, n/3, n/2$と鍵数が増加するにつれてqにおいてq_{kps}の割合は増加するため図 4 のように KPS2 のグラフに近づく。

5.3 耐盗難性の比較(KPS 部のみ)

3．で述べたように、提案方式ではランダム鍵事前格納方式部の要素鍵でリンク鍵の共有ができなかった場合、最低限の暗号通信をKPS 部に委ねる。これは、図3からわかるように、約3回に1回の確率でKPS部を用いて暗号化通信を行うことになる。しかし用いる秘密情報量は$l(<n)$であり、複数のノードに同じKPS 鍵プールが配布される状況が想定される。

以下では、可用性を保つためにKPS部を用いて暗号化通信を行うことを前提として、盗難ノード数cを増加させ、ランダム事前格納方式および有限幾何を用いた方式との危殆化確率q'を比較する。このq'は4.2に示すKPS部のみの場合のq_{kps}と同様である。なお、これは$K_{ran}(n_1)\cap K_{ran}(n_2)=0$のときランダム鍵事前格納方式部を除いた残りの通信数で評価するため、すべての方式においてノード数$n=33$とする。また、鍵の数は$l=1,5,10,20$とする。

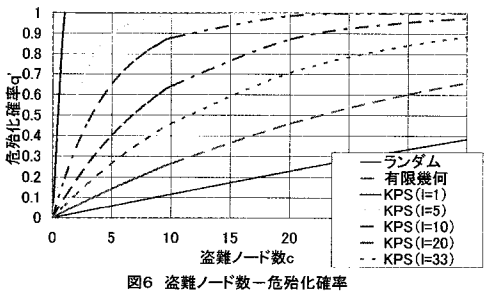

図6 盗難ノード数－危殆化確率

図6からわかるように、KPS部のみの場合、鍵数lにかかわらずランダム鍵事前格納方式より危殆化確率は高い。しかし、鍵数lの個数を変えることによって危殆化確率は変化させることができる。

以上から、$l=1$のとき従来のランダム鍵事前格納方式が可用性を持っていた部分に対してはほとんど同じ耐盗難性を実現するが、可用性を持っていなかった部分に対しては低い耐盗難性となることがわかる。また、lを増すにつれてランダム鍵事前格納方式が可用性を持っていた部分に対しては耐盗難性は減少していくが、可用性を持っていなかった部分に対しては逆に耐盗難性を向上させていけることがわかる。これによって、耐盗難性を目的に合わせて設定することが可能になる。

6 まとめ

本研究ではKPSの可用性とランダム鍵事前格納方式の安全性を利用した方式を提案し、ランダム鍵事前格納方式だけでは困難であった100%の可用性を実現した。耐盗難性は従来ランダム鍵事前格納方式が可用性を持っていた部分とそれ以外では異なるが、目的に合わせて設定することが可能である。これによって、センサネットワークの応用範囲を広げることができると思われる。

参考文献

[1]今井秀樹: “暗号のおはなし”,pp77-121

[2] W. Diffie , M. E. Hellman,: "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, Nov, 1976.

[3] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway: “Relations among notions of security for public-key encryption schemes” Extended abstract in Advances in Cryptology - Crypto 98 Proceedings, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed, Springer-Verlag, 1998.

[4] L.Eschenauer and V.D.Gligor: “A Key Management Scheme for Distributed Sensor Networks,” Proc.of the 9th ACM Conf.on Computer and Communications Securitey,pp.41-47,2002.

[5] H.chan, A.Perrig and D. Song: “Random Key Pre-distribution Schemes for Sensor Networks,” Proc. of the 24th IEEE Symp. On Securitey and Privacy,pp.197-213, 2003.

[6] 松本 律子,毛利 寿志,椙 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” 2006 年 暗号と情報セキュリティシンポジウム(SCIS2006),2006.

[7] 松本 律子,毛利 寿志,椙 勇一: “センサネットワークにおける有限幾何を利用した鍵事前格納方式” IEICE Rechnical Report ISEC2006-85(2006-09).

[8]Wenliang Du, Jing Deng, Yunghsiang S.Han, Pramod K.Varshney: “A Paerwise Key Pre-distribution Scheme for Wireless Sensor Networks”