社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (50)
2008－CSEC－ 40 (50)
2008／3／7

ネットワークのノード集合を分割管理するランダムキー事前分配法

伊勢 かおり† 阿部 公輝†

アドホックネットワークの攻撃対策である複合ランダムキー事前分配法 (q-composite random key pre-distribution, qRKP 法) では, 単一の鍵集合 (key pool) から各ノードに通信鍵 (key ring) を配布するためある通信路が破られた時に, 同じ鍵で別の通信路も破られる可能性がある. 本研究は,qRKP 法を基に, ノード集合をいくつかのグループに分割し, 互いに素な key pool を用いて管理する手法を提案する. 他のグループのノードとの通信路を確保するため, 隣接するグループの key pool からも鍵が分配されるノード (接続ノード) を用意する. 接続ノードの key ring の大きさが異なる 2 種類の適用例に対し, 攻撃シミュレーション実験を行った. その結果, 提案手法の方が qRKP 法に比べ盗聴確率が小さいことがわかった. また, グループ分割数が大きいほど盗聴確率が小さいことがわかった.

A Random Key Pre-distribution Scheme with Divided Key Management

Kaori Ise† and Kôki Abe†

q-composite Random Key Pre-distribution (qRKP), a countermeasure for ad-hoc network, distributes keys (key ring) taken from a unique key set (key pool) to each node. In qRKP, there is a chance that a key obtained from a compromised node can be used for tampering other secret links. In this paper, we propose a scheme based on qRKP. The scheme improves the security of ad-hoc network by dividing the node set into groups to each of which keys are pre-distributed from a disjoint key subset. Within each group of nodes connecting nodes are prepared for ensuring connection between nodes belonging to different groups. We conducted experiments to simulate attacks against two versions of the proposed scheme with different size of connecting nodes. The results revealed that the probability of eavesdropping on our proposed method is smaller than on the traditional qRKP method. It was also found that the lager is the number of divided groups, the smaller is the probability of eavesdropping.

1. はじめに

アドホックネットワークでは,2 つの端末は, 基地局を介さずに, その間にある別の通信端末を中継して通信する[1]. 被災地のような環境が不安定な場所でも通信が可能であるが, 端末がルーティングにも使われるため, 攻撃に対する脆弱性が問題となる.

攻撃への対策として、各ノードの設置前にランダムなキー集合を分配する手法, ランダムキーの事前分配 (Random Key Pre-distribution, RKP 法), が提案されている. RKP 法の基本形 key pool 法[2] に基づき, 様々なバリエーションが提案されている[3][4]. しかし, これらの手法では 1 つの鍵が複数の秘密リンクの形成に使われるため, 鍵を 1 つ奪われることで複数の秘密リンクが危険にさらされる可能性がある.

本研究では, ノード集合全体を 1 つの大きな鍵の集合で一括管理するのではなく, 複数のグループに分け, 各グループを互いに素な鍵の集合で個別に管理する手法を提案する. さらに, 各グループ内に複数個の接続ノードを用意し, 接続ノードに自グループの鍵集合からのみでなく, 隣接するノードグループの鍵集合からも鍵を分配する. この手法と従来法の耐攻撃性をシミュレーション実験により比較評価する.

以下では,2 章でアドホックネットワークのセキュリティ対策,3 章で従来法の説明, 4 章で提案手法の説明,5 章でシミュレーション実験, および結果と考察を述べる. 最後に 6 章でまとめる.

2. アドホックネットワークのセキュリティ対策

アドホックネットワークは無線通信を使用するため, データが盗聴されやすい. そのため攻撃受けてもデータを読まれないよう暗号化する必要がある. RSA[5] などの公開鍵暗号は, 共通鍵暗号よりも強いセキュリティ強度を持つが, 計算量が多いために電力消費も大きく, アドホックネットワークのように端末ノードのみで通

† 電気通信大学 情報工学専攻
Department of Computer Science, The University of Electro-Communications

信を行う際には不適切である. DES[6] などの共通鍵暗号は公開鍵暗号に比べてセキュリティ強度は劣るが, 少ない計算量で暗号化, 復号化が済む. しかし, この手法をそのままアドホックネットワークに適用するのは適切でない. たとえば, 全てのノード間で 1 つの鍵を共有すると, 各ノードが持つ鍵のデータが 1 つで済むために容量が少なくてすむが, 鍵を 1 つ奪われるだけですべての通信が盗聴される. 全てのノード間で異なる鍵を共有すると, 鍵を 1 つ奪われても奪われたノード間以外の通信を盗聴されないが, ノード数が大きいと必要な鍵の数も増え, ノードの容量を圧迫する.

RKP 法は対称鍵暗号の一種で, まず, あらかじめ大きな鍵の集合を用意し, そこから各ノードにそれぞれ鍵の束を配布する. 隣接ノード間で共通の鍵を探し出し, 通信路を作成する. 複合ランダムキー事前分配 (q-composite RKP, qRKP) 法[4] は, 通信路作成に使う共通の鍵を $q \geq 1$ 個に増やし, セキュリティ強度を向上させる. しかし,qRKP 法では一般に, 1 つの鍵が複数箇所で使われる可能性があり, 1 つの鍵が奪われることで複数の通信路が危険にさらされる.

3. 複合ランダムキー事前分配法

アドホックネットワークでは, ネットワーク運用中にネットワーク全体を監視することは難しく[1], 攻撃を完全に防ぐことは困難である. そこで, 攻撃の被害を軽減したり, 攻撃の手間を増大させるアプローチがとられ, その 1 つに RKP 法がある. はじめに, 基本方法とされているキープール法 (basic key pool scheme)[2] について, 次に提案手法の基となる qRKP 法について説明する.

3.1 ランダムキー事前分配法

s 個の鍵の集合を key pool S と呼ぶ. ノード i の ID ID_i を使って生成した乱数によって選ばれた m 個の鍵からなる S の部分集合 R_i を key ring と呼ぶ. ノード i はネットワーク構築時に配置される前に S から R_i を受け取る. 各ノードは配置後に, 隣接しているノードに対し, 互いの key ring から共通する鍵 (共通鍵) を見つけ出す. 共通鍵を用いて通信路 (秘密リンク) を形成する. S と m の大きさは, 任意のノード同士が秘密リンクを形成することができる確率 p と関係を持つ.

RKP 法は, 各ノード間で独立して共通鍵を決めるため, 敵に鍵を 1 つ奪われてもその鍵で全ての通信を盗聴されることはない. しかし秘密リンクを作るための鍵は 1 つなので, 盗聴の手間が比較的小さい.

3.2 複合ランダムキー事前分配法

qRKP 法[4] は, 秘密リンクに使用する共通鍵の数を $q \geq 1$ 個とし, それらをハッシュで 1 つにしたものを使用する. q が大きいほど秘密リンクを形成するための鍵の量が増えるため, 盗聴に必要な鍵の数が増えその分セキュリティ強度は増す. しかし, 任意のノード同士が秘密リンクを形成できる確率 p を一定の大きさに保つには,q が大きいほど key pool を小さくする必要がある. その結果奪われた鍵が秘密リンクに使われる可能性が上がり, セキュリティ強度が弱くなるという相反する性質を持つ. また, 全てのノードは同じ key pool から key ring を作成するため、ある秘密リンクが破られた時, 同じ鍵で別の秘密リンクも破られる可能性がある.

4. 提案手法

提案手法 ROKI☆ は,qRKP 法を基にする. 全てのノードが同じ key pool から key ring を作成するのではなく, ノード集合 N を $D(D \geq 2)$ 個のグループ $N_k(k = 1, ..., D)$ に分け, グループ N_k に key poolS_k を使用する. ($D = 1$ の場合は qRKP 法に対応する.) $S_k \cap S_l = \phi$, $k \neq l$, とする. こうすることで, グループ N_k で使用されている鍵は N_k 以外で使われることがなくなり, 鍵が奪われた際にデータが盗聴される確率が減ると考えられる.

しかし, このままではグループ間の通信路が確保できない. そこで, 図 1 に示すように N_k のノードの中に N_{k-1} の鍵を持たせるノード集合 NL_k と, N_{k+1} の鍵を持たせるノード集合 NR_k を用意し, それのノードを通して他のグループのノードとの通信路を確保する. $NL_k \cup NR_k = NC_k$ とする. NC_k $(k = 1, ..., D)$ に属するノードを接続ノードと呼ぶ. また, 接続ノードでないノードのことを通常ノードと呼ぶ.

N_k の通常ノードには key poolS_k から m 個の鍵を含む key ring を配る. NL_k (NR_k) に属するノードに key poolS_k,S_{k-1} $(S_k$,$S_{k+1})$ からそれぞれ m 個の鍵を含む key ring を配る手法を ROKI1, $m/2$ 個の鍵を含む key ring を配る手法を ROKI2 とする. ROKI1 の接続ノードの key ring の大きさは $2m$, ROKI2 の接続ノードの key ring の大きさは m となる.

☆ あるオンラインゲームにおいて, ひとつの道を数名が分担して守る技から名付けた.

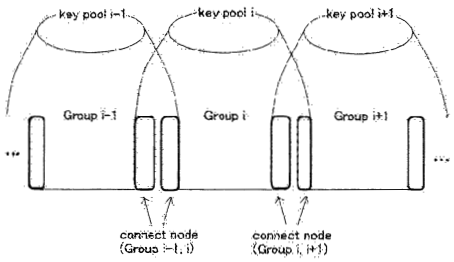

図 1 提案手法
Fig. 1 Proposed method.

5. 実　　験

5.1 目　　的

qRKP 法,ROKI1,ROKI2 の耐攻撃性をシミュレーション実験により調べる．攻撃としては, 文献[8] で行ったように, ノード単位, 鍵単位の攻撃を考える．また,ROKI1,ROKI2 に対しグループ数 D を変化させることによる耐攻撃性を調べる．

5.2 方　　法

ノード集合 N のグループ分けは $|N_1| = \cdots = |N_D|$(等分割) とする．s を正の整数として, グループ N_k の key poolS_k を $[1+s(k-1), s+s(k-1)]$ の範囲の整数の集合とする．S_k からランダムに鍵を選択し, 4 章で述べた方法に従って各ノードに分配する．

秘密リンクを作る際の共通鍵の数 q は 2 とする．ノード全体集合 N の任意のノード対全てにおいて秘密リンクを求め, その集合を L とする．

5.2.1 [実験 1] 鍵単位の攻撃とそれに対する耐性

あるノードの key ring 内のある鍵をランダムに選び奪う攻撃[8] を考える．これを攻撃 A と呼ぶ．攻撃回数 x_{A} を増やしていくことで, ノード間の秘密リンクの盗聴される確率 $y_{\mathrm{A}}(x_{\mathrm{A}})$ がどのように変化していくかについてシミュレーション実験を行い, 各手法を比較する．

$D = 4$,$m = 100$ とする．攻撃 A を x_A 回行うことで奪った鍵の集合を K_{A} とする．秘密リンク $r \in L$ を形成する共有鍵が全て K_{A} に含まれる時, そのリンクは盗聴される秘密リンクとして数える．盗聴される秘密リンクの集合を C_{A} とする．秘密リンクが盗聴される確率

$$y_{\mathrm{A}}(x_{\mathrm{A}}) = |C_{\mathrm{A}}|/|L| \tag{1}$$

を求める．

5.2.2 [実験 2] ノード単位の攻撃とそれに対する耐性

あるグループ内のあるノードをランダムに選び, そのノードが持つ key ring 内の鍵を全て奪う攻撃を考える．これを攻撃 B と呼ぶ．奪われるノードの数 x_{B} を増やしていくことで, ノード間の秘密リンクの盗聴される確率がどのように変化していくかについて, シミュレーション実験を行い, 各手法を比較する．また,key ring の大きさを変えて実験を行い, ノード 1 つが持つ鍵の量の違いによる耐攻撃性を調べる．

攻撃 B を x_B 回行うことで奪った鍵の集合を K_{B} とする．秘密リンク $r \in L$ を形成する共有鍵が, 全て K_{B} に含まれる時, そのリンクは盗聴される秘密リンクとして数える．盗聴される秘密リンクの集合を C_{B} とする．秘密リンクが盗聴される確率

$$y_{\mathrm{B}}(x_{\mathrm{B}}) = |C_{\mathrm{B}}|/|L| \tag{2}$$

を求める．

実験 2 では,key ring の大きさによる耐攻撃性の比較を行うために, $m = 100, m = 200$ の二通りの実験を行う．

5.2.3 [実験 3] グループ分割数の変化による耐攻撃性の比較

グループ分割数 D を変えることによる攻撃 A, 攻撃 B に対する耐攻撃性をシミュレーション実験により調べる．$D = 2, 4, 8, 10, 20$ の場合で実験 1, 実験 2 を行う．

5.3 条　　件

- key pool S_k の大きさ s は, 同一グループ内の任意の 2 つの通常ノードが秘密リンクを張ることのできる確率 p が 0.33 になるように調節する．任意の通常ノード対が i 個の共有鍵を持つ確率 $p(i)$ は次式で与えられる[4]．

$$p(i) = \frac{{}_{|S|}C_i \cdot {}_{|S|-i}C_{2(m-i)} \cdot {}_{2(m-i)}C_{m-i}}{\left({}_{|S|}C_m\right)^2} \tag{3}$$

  通常ノード対が秘密リンクを作る際の共通鍵の数は q であるので, 任意のノード対が秘密リンクを張ることの出来る確率 p は次式で与えられる．

$$p = 1 - (p(0) + p(1) + \ldots + p(q-1)) \tag{4}$$

  式 (4) より,p=0.33 となる時の s の値は $m = 100$ の時 $s = 8400$,$m = 200$ の時 $s = 35000$ となる．
- ノード数 n は 1000 とする．
- 接続ノード数は $|NL_k| = |NR_k| = 25$, すなわち $|NC_k| = 50$ とする．
- 乱数の生成には, 擬似乱数生成器 Mersenne Twister[9] を用いる．

5.4 結果と考察

5.4.1 [実　験　1]

攻撃 A の回数 x_{A} に対し, 秘密リンクが盗聴される

確率 $y_A(x_A)$ を図 2 に示す.

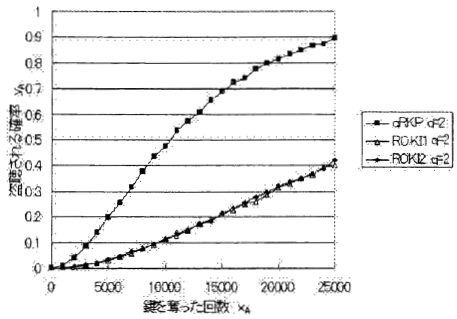

図 2 攻撃 A に対する耐性
Fig. 2 Resistivity against Attack A.

この結果より, 攻撃 A に対しての耐攻撃性は qRKP 法に比べ提案手法の方が優れていることがわかる. 特に, 原点付近での y_A の増加率が提案手法は低い. ROKI1 と ROKI2 の間に大きな差はない.

これは, 提案手法では通信鍵の重複を少量に抑えることが出来るため, 鍵 1 つ奪うことによるセキュリティ強度の低下度が qRKP 法に比べ小さく, その結果耐攻撃性に差がつくためと考えられる.

5.4.2 [実 験 2]

図 3,4 に, それぞれ $m = 100, 200$ の場合の $y_B(x_B)$ を示す.

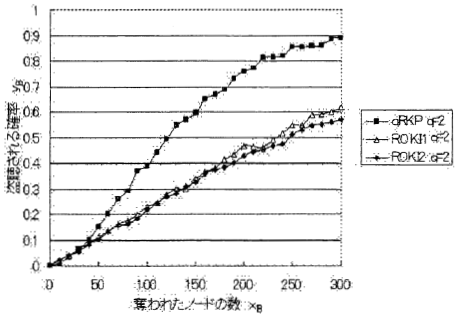

図 3 key ring=100 の時の攻撃 B に対する耐性
Fig. 3 Resistivity against Attack B(key ring=100).

qRKP 法は m が大きくなると耐攻撃性が上がる. これは,$m = 100$ の時 $s = 8400$ であるのに対し, $m = 200$ の時 $s = 35000$ であるため, 一回の攻撃 B で奪う鍵の数 $(=m)$ に対する key pool の大きさの比率が $m = 200$ の時のほうが小さいことによると考えられる.

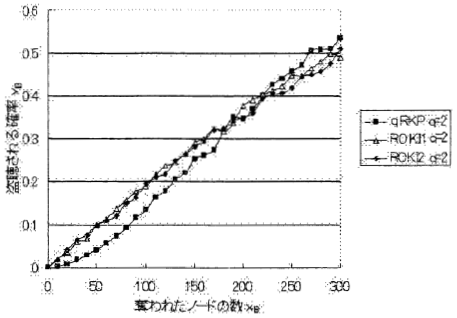

図 4 key ring=200 の時の攻撃 B に対する耐性
Fig. 4 Resistivity against Attack B(key ring=200).

一方, 提案手法は m が変化しても耐攻撃性はあまり変わらない. 提案手法は各グループによって異なる key pool を用いているため,qRKP 法に比べて奪った鍵が重複しにくい. そのため, 同じ x_B であっても, 実際に奪った鍵の key pool 全体に対しての割合が小さくならないと考えられる.

5.4.3 [実 験 3]

グループ分割数 D を変えた時の ROKI1,ROKI2 の攻撃 A に対する耐性を図 5,6 に示す. 図より,D が大きいほど盗聴確率が減る. これは, 攻撃によって奪った鍵は異なるグループでは秘密リンクを形成するのに使用できないため, グループ数が増えるほど奪われた鍵による盗聴確率が減ることによると考えられる.

また, 図 7 より $D = 4$ の時は ROKI1 と ROKI2 に大きな差はないが, $D = 20$ の時は ROKI2 より ROKI1 の方が盗聴確率が小さい. これは,ROKI1 の方が接続ノードの key ring が大きいために, 接続ノード間の秘密リンクを形成できる可能性のある鍵の数が多くなることによると考えられる.

グループ分割数 D を変えた時の ROKI1,ROKI2 の攻撃 B の耐性を図 8,9 に示す. 攻撃 A の時と同様,D が大きいほど盗聴確率が減る.

また, 図 10 より攻撃 A の時と異なり, $D = 4$ の時,ROKI1 より ROKI2 の方が盗聴確率が小さい. これは,ROKI2 の接続ノードの key ring の大きさが ROKI1 よりも小さいため, 接続ノードの鍵全体が奪われた時の被害が ROKI2 の方が小さくなるからと考えられる.

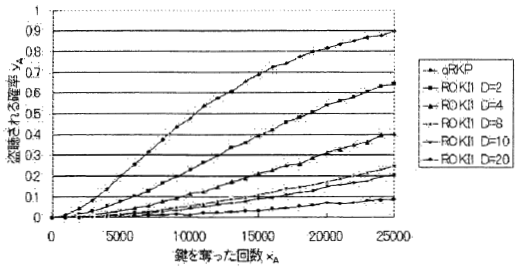

図 5 ROKI1 の攻撃 A に対する耐性
Fig. 5 Resistivity of ROKI1 against Attack A.

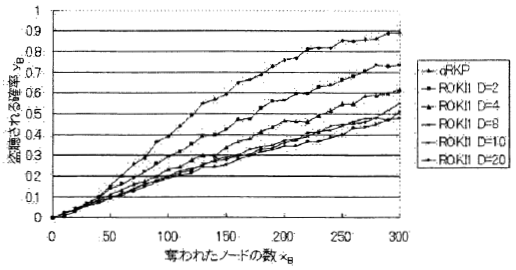

図 8 ROKI1 の攻撃 B に対する耐性
Fig. 8 Resistivity of ROKI1 against Attack B.

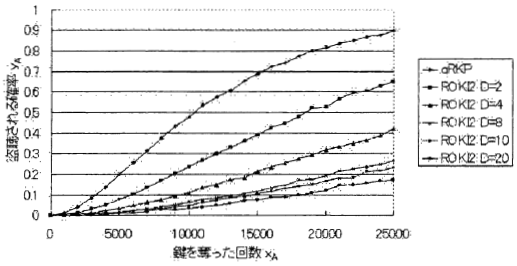

図 6 ROKI2 の攻撃 A に対する耐性
Fig. 6 Resistivity of ROKI2 against Attack A.

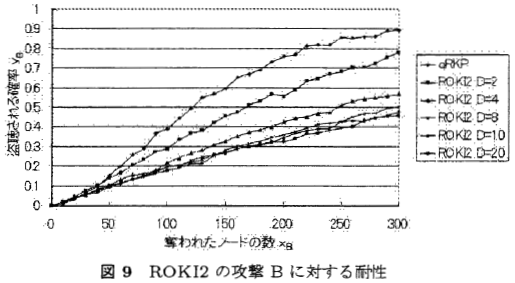

図 9 ROKI2 の攻撃 B に対する耐性
Fig. 9 Resistivity of ROKI2 against Attack B.

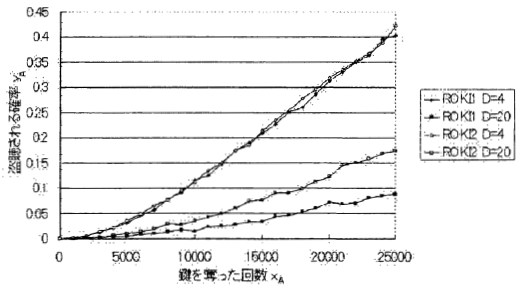

図 7 $D = 4, 20$ 時の攻撃 A に対する ROKI1, ROKI2 の耐性の比較
Fig. 7 Comparison of resistivity of ROKI1 and ROKI2 against Attack A for $D = 4, 20$.

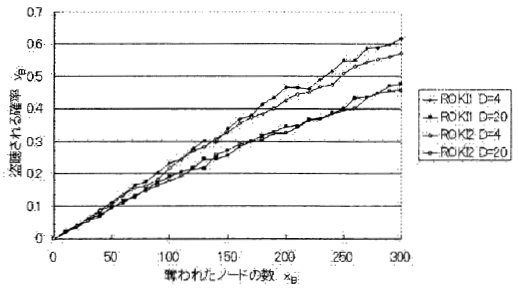

図 10 $D = 4, 20$ 時の攻撃 B に対する ROKI1, ROKI2 の耐性の比較
Fig. 10 Comparison of resistivity of ROKI1 and ROKI2 against Attack B for $D = 4, 20$.

6. おわりに

qRKP 法を基に, 互いに素な key pool を用いてノード集合を分割管理する手法 ROKI を提案した. 接続ノードの key ring の大きさが異なる 2 種類の手法 ROKI1,ROKI2 に対し, 鍵単位, ノード単位の攻撃シミュレーション実験を行った. その結果, 提案手法の方が qRKP 法に比べ盗聴確率が小さいことがわかった. また, グループ分割数が大きいほど盗聴確率が小さいことがわかった.

異なるグループの任意のノード間の接続性を考慮した評価実験については今後の課題である.

参 考 文 献

1) MANET, "Mobile Ad-hoc Networks," http://www.ietf.org/html.charters/manet-charter.html
2) L. Eschenauer and V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks," *Proc. the 9th ACM Conf. Computer and Communication Security*, pp.41-47, 2002.
3) J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," *Proc. Third International Symposium on Information Processing in Sensor Networks*, pp.259-268, Apr. 2004.
4) H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. IEEE Symposium on Security and Privacy*, pp.197-213, May 2003.
5) R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Sighatures and Public-Key Cryptosystems," *Communications of the ACM,* Vol.21 No.2, pp.120-126, Feb. 1978.
6) National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," *National Bureau of Standards, U.S. Department of Commerce* , Jan. 1977.
7) A. C. Chan, "Probabilistic Distributed Key Pre-distribution for Mobile Ad hoc Networks," *Proc. IEEE International Conference on Communications,* Vol.6, pp.3743-3747, June 2004.
8) 伊勢かおり, 阿部公輝, "複合ランダムキー事前分配法の耐攻撃性評価," 信学技報, Vol.107, No.29, AN2007-8, pp.41-45, May 2007.
9) "Mersenne Twister," http://www.math.sci.hiroshima-u.ac.jp/m-mat/MT/mt.html