単一経路木を用いるセンサーネットワークにおける匿名通信方式の提案

中村 彰吾 †　　堀 良彰 †　　櫻井 幸一 †

† 九州大学大学院システム情報科学府
819-0395 福岡県福岡市西区元岡 744
nakamura@itslab.csce.kyushu-u.ac, {hori, sakurai}@inf.kyushu-u.ac.jp

あらまし

現在，センサーネットワーク上での様々な匿名通信方式が提案されている．これらの方式は，任意の端末間での一対一通信を想定しているものが多い．ところが，現実にはネットワーク内の特定の端末に向けての多対一通信を行うような応用例も存在する．

そこで我々は，多対一通信を目指したセンサーネットワークにおける効率的な匿名通信を実現するための方式を提案する．また，その提案方式と既存方式とを比較することによって，本提案が大規模な多対一の単方向匿名通信を行う場合に，各端末が匿名経路を保持するのに必要な情報量という観点から優位性を持つことを示す．

Communication-Efficient Anonymous Routing Protocol for Single Path Tree Sensor Networks

Shogo Nakamura†　　Yoshiaki Hori†　　Kouichi Sakurai†

†Graduate School of Information Science and Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, Fukuoka 819-0395, JAPAN
nakamura@itslab.csce.kyushu-u.ac.jp, {hori, sakurai}@inf.kyushu-u.ac.jp

Abstract

Recently, there are anonymous routing protocols for sensor networks. These networks provide anonymous communication between arbitrary two nodes. So, all nodes can become source or destination in these protocols. However, there are also some multipoint-to-point sensor networks.

So, we propose a new anonymous routing protocol for such sensor networks. Moreover, we evidence superiority of our proposal by comparing the amount of information for anonymous routing with existing protocols.

1　序論

近年，多数のセンサー付き無線端末をエリア内に散在させ，端末間で情報のやり取りを行うセンサーネットワーク技術が発達している．このネットワークが抱える問題点の一つとして，悪意のあるトラフィック解析が行われやすいというものがある．この対策として匿名通信と呼ばれる，トラフィックを暗号化して通信を行う手法が挙げられる．

現在では，アドホックネットワーク上での匿名通信の実現を目指した様々な方式 [2] が提案されている．これら既存の方式では，任意のトポロジー構造を取りうる一般的なアドホックネットワークを想定している．しかし例えば，ツリー状のトポロジー構造を持ち，根に当たる部分が必ず終点となるようなネットワークであれば，任意の 2 端末間での通信を想定する必要はなく，常に根との通信を行うことだけを想定すれば良い．例として ARMR[1] では送受信端末の組ごとに匿名化に用いる鍵の情報が変化する．

そのため，ツリー状のトポロジー構造を持つネットワークにおいて同じ根に向けて異なる端末からメッセージを送信した際に，中継端末上で同じ宛先に向けての転送であっても異なる鍵の情報が必要となってしまうという欠点が存在する．

そこで我々は，ツリー状トポロジー構造を持つセンサーネットワークにおける効率的な匿名通信を実現するための通信方式を，既存の匿名通信方式と経路制御プロトコルをもとに提案する．また，提案した方式と既存の匿名通信方式とを比較することで，提案方式の優位性を示す．本稿では，各プロトコルが経路を構築，保持するのに必要な情報量に着目した上で，比較および考察を行う．

2　センサーネットワーク

2.1　ネットワークモデル

本稿では，エリア内に散在するセンサーが得た情報を，ある特定の端末に向けて集約させるようなネットワークを想定する．例として，近年注目されているスマートグリッドにおける，スマートメーターと呼ばれる機器のネットワークが挙げられる．これは自動検針機能付きの電力メーターであり，その機器が管轄する区画の使用電力を集計するためのものである．集計した情報は区画ごとに定められたゲートウェイ端末に送信され，ゲートウェイ端末はその情報を電力事業者などへ送信する．

このネットワークは消費電力を抑え，小規模な計算資源で動作が可能でなければならない．また，特定の端末に向けて多対一通信を行い，数千台規模で動作するという特徴を持つ．以上のことから，有効なネットワークモデルとしてある 1 つの特定の端末を終点として定め，その端末を根としたツリー上トポロジー構造を持つネットワークが考えられる．

これらを満足するようなセンサーネットワークにおける経路制御プロトコルとして，RPL(Routing Protocol for Low power and lossy networks)[3] と呼ばれるプロトコルが挙げられる．

2.2　RPL

RPL は IETF によって標準化が目指されている経路制御プロトコルの一つで，少ない制御メッセージでネットワークの安定化や再構築などを行うことができる．その特徴として，経路情報の保持に必要な情報量が一般的なものと比べて少ないことが挙げられる．

RPL ではネットワークを木構造を持つグラフとみなし，そのグラフの ID によって経路の区別を行う．グラフ ID は原則として各グラフの根にあたる端末ごとに異なるものを用意する．ただし，プロトコルの仕様上は 1 つのグラフに対して複数の根を持たせることも可能であるが，以下の説明では割愛する．

経路を構築する際には経路要求が起きなければならない．ネットワークに参加すしようとする端末は経路要求メッセージを送信し，メッセージはネットワークを通じて根端末まで到達する．その後経路構築メッセージをやり取りしながら各端末が rank と呼ばれる値を特定の評価指標に基づいて計算し，最適な経路を構築する．評価指標としてはホップ回数や送信電力などが考えられるが，今回の発表ではホップ回数を評価指標として考察する．経路の構築にあたって各端末はグラフ ID とグラフ上の自身の親の ID，および自身の rank の値を記憶しておけばよい．

実際に経路が構築されて通信を行う際には，該当する終点端末に対応したグラフ ID のエントリーを参照して，自身の親端末に向けて情報を送信する．また，自身の子端末から送られてきたメッセージについても，メッセージ内のグラフ ID を参照して転送先となる親端末を選択，転送する．なお，本稿では根端末が 1 つだけであると仮定しているため，グラフは 1 つだけしか存在しないものとする．

3　匿名通信プロトコル

情報の送受信者以外に送受信者情報を秘匿する通信のことを匿名通信という．この通信方式を用いることで，トラフィック解析攻撃を受けても送受信端末の情報が漏えいしない．

匿名通信の方式には大きく分けて Mix-net 方式と Onion 方式の 2 つが挙げられるが，今回は Onion 方式に着目する．これは通信路上で多重暗号化を行うことにより，通信にかかわるもの以外には経路情報を含むすべての情報が漏えいしないようにするという方式である．

以下では一般のアドホックネットワークにおける 2 つの既存の匿名通信プロトコルについてその特徴を説明する．

3.1 MASK[4]

MASK はプロアクティブな方式で経路構築を行う匿名通信方式である，そのため通信要求があった際には即座に通信を行うことができるという利点が存在する．

実際にデータを送信する際には，ペアによって異なる秘密鍵を用いてそれぞれのリンクを通過するたびに暗号化および復号処理を行う．

MASK が抱える問題点として，プロアクティブに経路を構築するため，定期的に端末間で経路制御メッセージのやり取りをしなければいけない点が考えられる．このことから，ネットワークの規模が大きくなればなるほど，制御メッセージのやり取りにおけるオーバーヘッドが飛躍的に大きくなってしまう．

3.2 ARMR(Anonymous Routing Protocol with Multiple Routes)

ARMR は MASK と異なり，通信要求を受けて経路の構築を行う．そのため MASK に比べて制御メッセージのやり取りに関するオーバーヘッドが少ないという利点が存在する．ただしその反面，通信要求発生後実際に通信を行うまでに遅延が発生するという欠点がある．

制御メッセージに含まれる送受信者情報は完全に暗号化され，実際に通信を行う際にも自身のアドレスとは無関係なハッシュ値を用いて経路を管理するため，いかなる状況においてトラフィック解析を行われても攻撃者に情報が漏れることはない．

しかしこのハッシュ値は始点と終点とで共有するものであるため，同一の端末に向けて異なる端末が通信を行う際に，途中から経路が合流してしまうようなトポロジー構造の場合，合流後の経路上では同じ終点端末へ向かう経路であっても始点端末の数だけハッシュ値および鍵情報を保持する必要があるという欠点を持つ．

4 提案方式

本稿で想定しているネットワークには，外部ネットワークに情報を送信するゲートウェイ端末のネットワーク上の位置情報が攻撃者に漏れてしまうと，その端末が DoS などの攻撃を受ける危険性がある．そのため，対策として匿名化を行うことが考えられる．

もちろん，このネットワークはアドホックネットワークの一種であるため，既存の方式を適用することも可能である．しかし，MASK を適用する場合は大規模なネットワークゆえに大きなオーバーヘッドが発生すると考えられ，ARMR を適用する場合はツリー構造の上位，つまり根に近いほうの端末が冗長に経路情報を保持しなければならなくなってしまう．そこで我々は，このようなネットワークが要求する事項に特化した匿名通信方式を提案する．以下に提案方式の概要を示す．本提案では既存方式と RPL をもとに，想定しているネットワークモデルに適した匿名通信方式を考える．

4.1 前提

まず，全ての端末はある端末に向けてパケットを送信するとする．つまりネットワーク内のすべての端末はある端末に向けられたものである．その端末はこのネットワークのトポロジーにおける根となる．

次に，根端末は 1 組の公開鍵と秘密鍵の組を保有し，公開鍵はすべての端末に公開されているとする．

そして，全ての端末はあるハッシュ関数を共有しているとする．また，2 つの値を共有しているとする．このハッシュ関数は経路要求時に，2 つの値は経路構築時に使用される．

最後に，各端末はそれぞれ 2 つの値 x と y を保有しているとする．この値は Diffe-Hellman の鍵共有方式を行う際に使用される．

なお，本稿ではネットワーク内には存在せず，端末間でやり取りするパケットを傍受することのみを行うものとする．つまり，攻撃モデルとしては傍受したパケットの解析による送受信者情報の取得のみを取り扱うこととし，ネットワーク内に侵入しての中間者攻撃などは考慮しないとする．

以下では始点端末 S からある根端末 D にむけて経路を構築し通信を試みると仮定する．

4.2 匿名経路要求

まず，S は D の公開鍵によって S の情報 (I_S)，ワンタイムキー (O) および D の情報 (I_D) を暗号化する．さらに，S は乱数 (r) を生成し，そのハッシュ値 (H_S) を求める．その上，S は r を O で暗号化する (C).

次に，S は経路要求メッセージ (RREQ) をブロードキャストする．RREQ には I_S，O，I_D，r，H_S および C が含まれている．RREQ を受け取った端末は自分の親端末に向けて RREQ を転送する．

以下繰り返すことで，D が RREQ を受信する．その後，D は I_S，O および I_D を自身の秘密鍵で復号する．I_D が自身の情報と一致すれば次の処理を行う．そうでなければ RREQ を破棄する．

最後に，D は r のハッシュ値を計算し (H_D)，H_S と比較する．H_D と H_S の値が等しければ，その経路要求を受理し経路構築を行う．

このフェーズでは，攻撃者が RREQ を盗聴することができても I_S と I_D を知ることはできない．よってこのフェーズにおける匿名性は満たされている．

4.3 匿名経路構築

まず，D は経路応答メッセージ (RREP) をブロードキャストする．RREP にはグラフ ID(I_G)，グラフシーケンスナンバー (N_G)，送信端末のランクおよび送信端末の y が含まれている．端末が RREP を受信すると，自身の経路表を参照して I_G，N_G および rank を比較する．そしてもしも RREP の情報が初見のもの，最新のもの，あるいはより良いものであるならば，経路表を更新するここでより良い RREP とは RREP における rank が自身の経路表における rank よりも 2 以上小さいことを意味する．

次に，RREP を受信して経路表を更新した端末は，RREP を送信してきた自身の親端末と鍵を共有する．そのため自身の y を親端末に向けてユニキャストし，自身の x と RREP 内の親端末の y から親端末と共有する鍵を生成する．また，自身の子にあたる端末から y を受信した際には，自身の x と子端末の y から子端末と共有する鍵を生成する．

そして，RREP を受信した端末は再度 I_G，N_G，自身のランクの値および自身の y を含んだ RREP をブロードキャストする．

この繰り返しにより，全ての端末は I_G，N_G，親の情報 (I_P)，自身のランク (R)，親との共通鍵 (K_P) および子との共通鍵 (K_C) を含んだ経路表を保有することができる．

このフェーズでは，攻撃者は D の情報 (I_D) を得ることができない．また，経路は全ての端末のために作られるため，経路要求をした端末 S が何なのかを知ることはできない．よってこのフェーズにおける匿名性も満たされている．

4.4 匿名パケット送信

まず，S は K_P によって送信するパケットのすべてのフィールドを暗号化し，ブロードキャストする．もしも受信した端末が D の親 (P_S) でなければ，このパケットは復号できない．そのためその場合はそのパケットを破棄する．

次に，P_S が S からのパケットを受信すると，P_S は自身の K_C でそのパケットを復号する．その後，P_S は自身の K_P によって再度そのパケットを暗号化し，ブロードキャストを行う．

この繰り返しにより，D は S から送られてきたパケットを受信することができる．

このフェーズでは，攻撃者はどの時点でも S からのパケットを読み取ることができない．よってこのフェーズにおける匿名性も満たされている．

なお，提案方式も先に紹介した既存方式も，匿名性を得るのに必要な計算量は同程度である．これはこれら 3 つの方式がともにホップバイホップで暗号化および復号化を行うためである．よって，これらの性能を比較する際には，経路構築の際にどの程度のコストがかかるかという点に着目する必要がある．具体的には，経路構築までに時間，経路保持に必要な記憶容量などの観点から評価を行うことになる．

5 評価

本稿で提案した方式と既存方式とを，各端末が保有しなければならない鍵数という観点から比較することで，各端末の記憶容量へのコストを評価する．

5.1 完全二分木を想定した解析

まず最初に，経路木として木構造の典型的なものである完全 n 分木を想定して，鍵数の解析および比較を行う．一般にネットワークを n 分木構造にすることで，多数の端末を少ない段数で収容することが可能となる．しかし n が増加すると各端末における隣接端末数が増加するため，保持しなければいけない鍵数が増加する．そこで n を 2 として二分木を想

定することで，各端末が保持しなければならない鍵数を抑えたうえで，かつ段数も抑えること可能となる．また，完全二分木は木構造としても単純な構造をしており，ネットワーク特性を考える上で特徴の抽出がしやすいモデルであると考えられる．

以上より，以下では完全二分木を想定して，鍵数の解析および比較を行う．

表 1: 完全二分木における鍵数

	MASK	ARMR	提案方式
公開鍵	なし	1 組	1 組
共通鍵	$2^{n+1}-4$	$\sum_{i=1}^{n} i2^i$	$2^{n+1}-4$
鍵数	$O(1)$	$O(n^2)$	$O(1)$

トポロジーとして完全二分木を想定したときの，各プロトコルにおける鍵数を表 1 に示す．

ARMR は他の 2 つのプロトコルに比べて非常に多くの鍵を各端末が保持しなければならない．これは各端末が自身を経由する経路ごとに 2 つの鍵 (前端末用の鍵と次端末用の鍵) を保有しなければならないためである．その際，仮に同じリンクを使用することになったとしても，共有する鍵は異なるものを使用することになっている．そのため，端末数が増加すればするほど，根端末に近い端末ほど多くの鍵を隣接端末と共有しなければならない．

MASK および提案方式では，隣接端末と共有する鍵の数は 2 つだけで済む．しかし MASK においては，自身の全ての隣接端末と鍵を共有しなければならない．そのため，実際には表 1 のものよりも多くの鍵を共有することが予想され，その分鍵数のオーバーヘッドが発生する可能性がある．一方，提案方式では各端末は必要最小限の鍵の共有しか行わないためそのような鍵数のオーバーヘッドは発生しない．

表 2: シミュレーション環境

NS Version	2.34
Channel Type	Channel/ WirelessChannel
Radio-propagation	Propagation/ TwoRayGround
Network Interface	Phy/ WirelessPhy
MAC	802.11
Interface Queue	Queue/DropTail/ PriQueue
Link Layer	LL
Antenna Type	Antenna/ OmniAntenna
Queue Size	100
Comm. Range	150

5.2 シミュレーション

前小節では経路木として完全二分木を想定した上で，解析的に各プロトコルの比較を行った．本小節では実際にネットワークシミュレーターの 1 つである ns-2.34 を用いてシミュレーションを行い，各プロトコルの比較をより現実に近い場合において行う．表 2 に本稿におけるシミュレーション環境を示す．

5.2.1 端末密度

本提案方式が大規模ネットワークにおいて優位性を持つことを示すために，数百から数千個の端末数でのシミュレーションを行う．しかしその際，シミュレーション環境として固定すべき値はネットワークエリアの大きさではなくそのネットワークを構成している端末の密度である．なぜなら，同じ大きさのエリア内で端末数を増加させたとしても，エリアの端から端まで通信をする際に必要な中継端末の数は変化しないためである．よって，端末数を変化させる際には，端末の密度を変化させないよう同時にネットワークエリアも変化させるべきである．

シミュレーションの際に用いる端末密度を決定するため，ネットワークエリアを 1km 四方に固定した上で端末数を変化させ，RPL を用いて経路制御を行った．この実験から得られたネットワーク内の Rank の分布を図 1 示す．ただし，これらの値は根に当たる端末を原点に固定し，各端末数で 3 度の実験を行って得られた結果の平均値である．

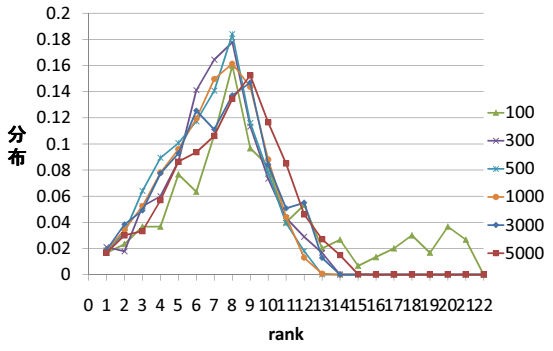

図 1: Rank の分布

端末数が 100 の場合のグラフを見てみると，ほかのグラフに比べてピークの値が目立たず，形状も異質なものとなっている．このことから，端末数 100 の場合はネットワークの構造が不安定になりやすいと考えられる．これは，エリアの大きさに対して端末の数が少なすぎるため，発生した乱数によるネットワークの構造のばらつきが大きいためだと予想される．一方，端末数が 3000 を超える場合もグラフの形状がそれまでのものに比べて変化している．これは，エリアの大きさに対して端末数が多すぎるため，各端末の隣接端末数のばらつきが大きくなるために，ネットワークの構造が不安定になると考えられる．端末数が 300 から 1000 の場合はグラフの構造が似通っている．特に 500 の場合と 1000 の場合とでは差がほとんど見受けられない．このことから端末数を 500 以上に増加させてもネットワークの構造に大きな変化は起きないと考えられる．

以上のことから，1km 四方のネットワークエリアにおける最適な端末数を 500 個とし，端末密度を $500/km^2$ として以下の実験を行う．

5.2.2 鍵数

前小節で得られた端末密度を用いて，端末数を 100 から 5000 まで変化させた際に各端末が保持する鍵数の平均値を，シミュレーションによって得られたトポロジーから求める．今回も根に当たる端末を原点に固定して 3 回の実験を行ったうえで，得られた結果の平均値を用いて考察を行う．

表 3: 各端末の平均保有鍵数

n	Our Protocol	ARMR	MASK
100	1.98	3.13	15.84
300	1.99	5.35	20.65
500	2.00	6.94	22.29
1000	2.00	9.55	25.77
3000	2.00	16.30	29.99
5000	2.00	20.84	30.94

各端末の平均保有鍵数を表 3 と図 2 に示す．

先に示したように，ARMR では自身を経由する経路があればある程多くの鍵を保持しなければならず，MASK では隣接端末の数だけ鍵を保持しなければならない．一方，提案方式では自身の親および子と鍵を共有するだけであるため，既存方式に比べて保有すべき鍵の個数が少ない．つまり，既存方式

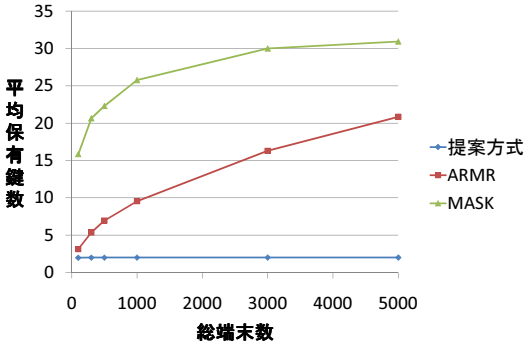

図 2: 各端末の平均保有鍵数

を用いれば経路を保持する際に要求される記憶容量を抑えることが可能となる．これはセンサーネットワークにおいて非常に有益な特徴であるといえる．

6 結論および今後の課題

本稿では単一経路木を用いるセンサーネットワークにおける効率的な匿名通信方式を提案した．さらに，既存の 2 つのプロトコルと比較することで，その提案方式の優位性を示した．

今後の課題としては，通信遅延や経路構築までにかかる時間などのパフォーマンスレベルの比較を行うことが挙げられる．

参考文献

[1] Ying Dong, Tat Wing Chim, Victor O. K. Li, S. M. Yiu and C. K. Hui. “ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks”, Ad Hoc Networks 7, pp. 1536-1550, 2009.

[2] Shino Sara Varghese and J. Immanuel John Raja. “A Survey on Anonymous Routing Protocols in MANET”, RECENT ADVANCES in NETWORKING, VLSI and SIGNAL PROCESSING, pp. 88-92, 2010.

[3] Jeonggil Ko, Terzis A., Dawson-Haggerty S., Culler D.E., Hui J.W. and Levis P. “Connecting Low-Power and Lossy Networks to the Internet”, IEEE Communications Magazine, Vol. 49, Issue 4, pp. 96-101,2011.

[4] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang. “MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, pp. 2376-2385, 2006.