情報処理学会論文誌 Vol.53 No.9 2245–2253 (Sep. 2012)

多対一通信を行うセンサネットワークのための単一経路木を用いる匿名通信方式の提案

中村 彰吾[1,†1] 堀 良彰[2,a)] 櫻井 幸一[2]

受付日 2011年11月30日, 採録日 2012年6月1日

概要：現在，無線アドホック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．そのような環境では特定の端末と任意の端末間での経路を考慮するだけでよい．しかし既存の匿名通信方式では安全性のみを追求しており，効率的に動作することまでは考慮されていない．我々は，多対一通信を目指したセンサ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，既存の方式を基に提案する．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，効率面での優位性を持つことを示す．

キーワード：匿名通信，経路制御プロトコル，多対一通信，無線センサネットワーク，ネットワークセキュリティ

Anonymous Single Path Tree Routing Protocol for Multipoint-to-point Wireless Sensor Networks

Shogo Nakamura[1,†1] Yoshiaki Hori[2,a)] Kouichi Sakurai[2]

Received: November 30, 2011, Accepted: June 1, 2012

Abstract: In recent years, there are anonymous routing protocols for wireless ad-hoc networks. These protocols provide anonymous communication between an arbitrary pair of nodes. However, there are also some multipoint-to-point sensor networks. In those environments, we have to consider all routes not between an arbitrary pair of sensor nodes but between an arbitrary one sender node and a specific destination node. These existing protocols consider to only security, so nodes may not be able to work efficiency in those environments. We propose a new anonymous routing protocol for such multipoint-to-point sensor networks based on efficient routing protocols and existing anonymous routing mechanisms. Moreover, we evidence superiority of our proposal by comparing with that of existing protocols, and show that our protocol can establish the anonymous route faster than existing ones and reduce the information for routing from existing ones.

Keywords: anonymous communication, routing protocol, multipoint to point communication, wireless sensor network, network security

1. 序論

近年，多数のセンサ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とりを行うセンサネットワーク技術が発達している．このネットワークがかかえる問題点 [1] の1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通信方式がある．

[1] 九州大学大学院システム情報科学府
Graduate School of ISEE, Kyushu University, Fukuoka 819–0395, Japan
[2] 九州大学大学院システム情報科学研究院
Faculty of ISEE, Kyushu University, Fukuoka 819–0395, Japan
[†1] 現在，三菱電機情報ネットワーク株式会社
Presently with MITSUBISHI ELECTRIC INFORMATION NETWORK CORPORATION
[a)] hori@inf.kyushu-u.ac.jp

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，任意のトポロジ構造をと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，センサネットワークの本来の目的である複数の観測点からの情報を収集するという観点から考えると，任意の端末間の一対一通信を想定するよりも，複数の端末がある端末に向けて通信を行うという多対一通信を想定するべきである．このように多対一通信を行う際のネットワークモデルとしては，ツリー状のトポロジ構造を持ち，根にあたる部分が必ず終点となるようなモデルが考えられる．この場合，任意の 2 端末間での通信を想定する必要はなく，つねに根との通信を行うことだけを想定すればよい．

そこで我々は，多対一通信を行うセンサ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，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および時間に着目したうえで，比較および考察を行う．

2. センサネットワーク

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，スマートメータと呼ばれる機器のネットワークがあげられる．これは自動検針機能付きの電力メータであり，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．以上の特性を満足するようなセンサ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] がある．

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 1 つで，通信量を抑えながら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記憶域が，AODV や OLSR などの一般的なアドホックネットワークにおける経路制御プロトコルより少なくて済むことがあげられる．RPL ではネットワークを木構造を持つグラフと見なし，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．プロトコルの仕様上，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ルート端末まで到達する．その後経路構築メッセージをブロードキャストしながら各端末がランク（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，本稿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 を記憶する．

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 のエントリを参照して，自身の親端末に向けてメッセージを送信する．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，本稿ではルート端末が 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．以下では一般の一対一通信を想定している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，プロアクティブな方式とは，任意の端末からのどのような経路要求にも応えられるように，考えうる全経路の構築をあらかじめ行っておくという方式である．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ホップバイホップで暗号化および復号処理を行う．

MASK がかかえる問題点として，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とりをしなければなら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とりにおけるオーバ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）[5]

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とりに関するオーバ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（Deny of Service，サービス停止）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．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ヘッドが発生すると考えられ，ARMR を適用する場合は宛先に近い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．本稿では既存方式と RPL をもとに，多対一通信を行う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，すべての端末はある端末に向けてメッセージを送信するとする．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における共通の宛先となる．以下，この端末のことをルート端末と呼ぶ．次に，ルート端末は 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．また，各端末はある巨大な素数 p と p に対するある原始根 g の組 (g, p) を共有しているとする．これらの値は経路構築時の Diffie-Hellman 鍵共有を行う際に使用される．最後に，各端末はそれぞれ独自の 2 つの値（$x, y = g^x \bmod p$）を保有しているとする．この値も Diffe-Hellman の鍵共有方式を行う際に使用され，x を秘密値，y を公開値と呼ぶ．以下では始点端末 S からあるルート端末 D に向けて経路を構築し通信を試みると仮定する．

4.2 経路要求

まず，送信者 S は宛先 D の公開鍵によって S の情報 I_S および D の情報 I_D を暗号化する．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 には前述のとおり暗号化された I_S および I_D 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 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経路要求を受理する．そうでなければ RREQ を破棄する．

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 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 IDI_G，グラフシーケンスナンバ N_G，送信端末の Rank および公開値 y が含まれている．なお，これらの値から端末のネットワークアドレスなどを知ることはできないため，これらの値には暗号化を行わない．端末が RREP を受信すると，自身の経路表，つまりメッセージ転送に必要な情報をまとめた表と RREP の内容とを比較する．経路表内には I_G，N_G および Rank が記録されている．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，初見の RREP とは RREP における I_G が自身の経路表に登録されていないことを意味する．最新の RREP とは RREP における N_G が自身の経路表における N_G よりも大きいことを意味する．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．なお，もしも受け取った RREP における Rank が自身の経路表における Rank よりも 1 だけ小さい場合は，経路表を更新しても自身の Rank が変化しないため，自身より下位の，つまり自身の子端末以下の効率性の向上を見込むことができない．よって，Rank を経路表更新の指標とする際には，自身の Rank よりも 2 以上小さいことが必要となる．

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しながら，RREP をフラッディングする．ここでは便宜上，RREP の送信端末を D，受信端末を F とし，それぞれの秘密値 x と公開値 y を x_D，x_F および y_D，y_F とする．F が D から RREP（Rank = 0）を受信して経路表を更新すると，F は自身の x_F と RREP 内の y_D から D との公開鍵を生成する．その後，F が自身の子に向けて送信した RREP（Rank = 1）を D が受信した際に，自身の x_D と RREP 内の y_F から F との公開鍵を生成する．この繰返しにより，すべての端末は

I_G，N_G，親の情報（I_P），自身の Rank（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，経路はすべ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 メッセージ送信

まず，S は K_P によって送信するメッセージ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，このメッセージは復号できない．そのためその場合はそのメッセージを破棄する．

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

この繰返しにより，D は S から送られてきたメッセージ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 からのメッセージ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，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，実際に通信を行う際の各端末上での通信遅延は同程度であると考えることができる．

5. 評価

5.1 攻撃者モデル

評価に先立って攻撃者のモデルを定義する．今回は攻撃者がネットワークの内部には存在しないものと仮定する．攻撃者はセンサよりも高い計算能力を持っており，無線通信路上のトラフィックを盗聴，解析を試みるものとする．これをトラフィック解析攻撃と呼び，本稿では特にメッセージ長解析，内容解析，振舞い解析の 3 種類の攻撃を取り上げる．なお，攻撃者がネットワーク内に入ってメッセージの内容を盗み見るような中間者攻撃に関しては，ネットワーク参加時に認証を行うという方法で回避できていると仮定している．

5.2 匿名性評価

5.2.1 評価

表 1 は我々の提案方式と既存方式とを比較したものである．匿名性の評価を行ううえで必要な要件に関してはすでに先行研究で議論がなされており，我々もそれにのっとった考察を行う [6], [7]．ID 秘匿性とは，通信にかかわっている端末の ID が，トラフィックを解析するだけでは知ることができないという特徴のことである．今回は送信者，受信者，中継者の 3 要素について，それぞれ ID 秘匿性があるかどうかを評価した．リンク不能性とは，同一の端末による複数の動作について，それぞれの動作が同一のユーザによるものであるかどうかということを判断できないという特徴のことである．今回はトラフィック解析攻撃の中でもメッセージ長解析，内容解析，振舞い解析の 3 種類の攻撃に対して，それぞれリンク不能性があるかどうかを評価した．検出不能性とは，ある端末がネットワーク内に存在するかどうかを，第三者，つまり攻撃者によって判断できないという特徴のことである．偽名性とは，あるものを識別する際にそのものの本来の名前を用いるのではなく，それと関係のないものを識別子として用いているという特徴である．

表 1 匿名性の要素
Table 1 The elements of anonymity.

匿名性の特性	提案方式	ARMR	MASK
送信者 ID 秘匿性	√	√	√
受信者 ID 秘匿性	√	√	
中継者 ID 秘匿性	√	√	√
メッセージ長のリンク不能性	√	√	√
内容解析へのリンク不能性		√	√
振舞いのリンク不能性		√	√
検出不能性	√	√	√
偽名性	√	√	√
始点–終点間の暗号化	√	√	√

最初に，ID 秘匿性の有無について述べる．提案方式では送信者情報と受信者情報をリンク，つまり親子の通信路ごとに異なる鍵で暗号化している．そのため，単にメッセージを解析しただけでは送受信者の ID を判別することはできない．また，本提案方式ではユニキャストを行わないため，中継者の ID を通信時に使用することはありえない．よって攻撃者がどれだけメッセージを解析したとしても，中継者の ID が知られることはない．以上のことから，通信にかかわるすべての端末の ID 秘匿性が保たれているといえる．

次に，メッセージ長のリンク不能性の有無について述べる．メッセージ長解析攻撃とは，複数のメッセージのメッセージ長を解析，比較することで，それらの関連性の有無を判断するという攻撃のことである．今回想定している環境は，特定の端末が複数の観測点からの情報を収集するというものである．そのため，各端末の役割は，ルート端末を除いてすべて同等のものである．このことから，通常の状態であればメッセージ長が著しく他と異なるような通信が発生することはほとんどないと考えてよい．よって，ホップバイホップで暗号化する際に，考えうる最大のメッセージ長になるようメッセージをパディングし，これに対してブロック暗号を使用することで，つねに一定の長さの

メッセージ長で通信することが可能になる．以上より，攻撃者が複数のメッセージを受信したとしても，それらはすべて同じメッセージ長となると考えることができる．これにより，たとえ関連性のある複数のメッセージを攻撃者に解析されたとしても，それらが本当に関連性があるのかどうかをメッセージ長から判定することは難しく，ゆえにメッセージ長のリンク不能性が保たれているといえる．

続いて，内容解析へのリンク不能性の有無について述べる．内容解析攻撃とは，同一の送受信者情報を持つ複数のメッセージに対して，攻撃者がそれらの中から類似した文字列パターンがあるかどうかを解析することで，それらの関連性の有無を判断するという攻撃のことである．本提案方式ではリンクごとに異なる鍵を使用するため，1 度の通信では内容解析攻撃を受けても関連性の有無を判断することはできない．しかし，ある端末が自身の情報を複数回にわたって送信した場合，使用する鍵が同一であるため，送受信者に関する情報はまったく同じ暗号文になってしまう．そのため，そのようなメッセージを攻撃者が盗聴することができた場合，それらの関連性の有無を判断することができてしまう．よって現時点では本提案方式において内容解析へのリンク不能性が保たれているということはできない．なお，比較対象としている既存方式ではマルチパスルーティングを行うことで，内容解析へのリンク不能性を保っている．しかし本提案方式ではトポロジとして木構造を構築するため，その方針をとることができない．

さらに，振舞いのリンク不能性の有無について述べる．振舞い解析攻撃とは，端末の挙動を長期的に観測することで，その端末がどのような端末なのかを判断するという攻撃のことである．本提案方式では木構造のトポロジを構築するため，必然的にルートとリーフとでは挙動が異なってしまう．ルート端末はネットワーク内のすべての端末からメッセージを受け取ることになる．そのため，攻撃者から見て最も頻繁にメッセージを受信しているものがルートであると推測することが可能となってしまう．また，リーフ端末は逆にいっさいの中継を行うことがない．そのため，攻撃者から見て最もメッセージのやりとりの少ないものがリーフであると推測することが可能となってしまう．このことから，振舞いのリンク不能性も保たれているということはできない．なお，前述のとおり，比較対象としている既存方式はマルチパスルーティングを行うため，このようなことは起きない．これは木構造のトポロジに特有の問題であると考えられる．

最後に，検出不能性および偽名性の有無について述べる．本提案方式ではルート端末以外が自分の ID に関する情報をメッセージに含めるという状況が存在しない．また，ルート端末の識別には端末の ID ではなくグラフの ID を用いるが，これはルート端末の ID に依存しない．よって攻撃者からみるとある端末が存在するかどうかを検出することはできず，検出不能性は保たれているといえる．また，先に述べたとおりルート端末以外の端末をネットワーク上で識別する必要はなく，識別が必要なルート端末に関しては自身の ID に依存しないグラフ ID を用いることから，偽名性も保たれているといえる．

5.2.2 改善手法の考察

前述のとおり，現時点での我々の提案方式には内容解析攻撃および振舞い解析攻撃に対する耐性がない．そこで対策手法を検討する必要がある．

まず，内容解析攻撃に関する対策を考える．内容解析攻撃が成功するための条件としては，以下の 2 点が考えられる．

- 同一の送信端末からのメッセージ内にはつねに共通する情報が存在する．
- 異なる送信端末からのメッセージ内には共通する情報が存在しない．

つまり，以下のいずれかを達成することができればよい．

- 送受信者が同一のメッセージであっても共通する情報が含まれないようにする．
  - つねに各端末の ID を変化させる．
  - 毎回の通信時に使用する鍵を変更する．
- すべての送信端末からのメッセージを同一の内容にする．

ただし，一般に各端末の ID はネットワークアドレスを想定することが多く，頻繁に変更することは難しい．また，メッセージの内容は各センサのセンシングの結果であるため，すべてのメッセージの内容を一致させることは不可能である．よって本稿では，毎回の通信時に使用する鍵を変更するという方式を検討する．今回は，アプリケーションとしてスマートメータを想定する．これは通信機能を持った電力計であり，将来スマートグリッドが普及していくうえで必須となるアプリケーションの 1 つである．スマートメータの場合は管轄する施設などにおける消費電力量を定期的に電力事業者に送信する．ただし，外部ネットワークにつながっている端末はエリアに 1 台だけ存在し，それ以外の端末は無線通信によって自身の情報をその端末に伝える．今回はその無線通信網を匿名化すると考える．このとき，特定のタイミングで自身の持っている消費電力に関する情報を送信するとき以外は，各端末は待機状態になっている．つまり，通信を行っていない待機時間中に鍵を再生成および再共有することにより，送受信者情報を暗号化した結果を毎回異なるものとすることができる．これにより，スマートメータなどの定期的な通信を行うようなアプリケーションに限定すれば，内容解析へのリンク不能性を得ることができる．ただし，この方式を用いて提案手法の匿名性を向上させた場合，毎回の通信タイミングが終了するごとに後述の経路構築時間分の通信が発生するという問題点がある．

表 2 完全二分木における平均鍵数
Table 2 The average number of keys on complete binary tree.

	MASK	ARMR	Our Protocol
Symmetric Key Cryptosystem	more than $2^{n+1}-4$	$\sum_{i=1}^{n} i2^i$	$2^{n+1}-4$
The Number of Keys Per Node	$O(1)$	$O(n^2)$	$O(1)$

次に，振舞い解析攻撃に関する対策を考える．振舞い解析攻撃が成功するための条件としては，以下の 2 点が考えられる．

- 他の端末に比べて振舞いが特徴的な端末が存在する．
- 各端末の役割がつねに変わらない．

つまり，以下のいずれかを達成することができればよい．

- 特徴的な振舞いをしていることを攻撃者から見て気付くことができないようにする．
  - 特徴的な動きをする端末に他の端末が動きを合わせる．
  - 特徴的な動きをする端末が他の端末の動きに合わせる．
- 各端末の役割を変化させる．

このうち，特徴的な動きをする端末が他の端末の動きに合わせるという方式を検討する．ここでもスマートメータをアプリケーションとして想定する．ただし今回は，スマートメータの特徴よりも木構造のトポロジという特徴に着目して検討する．このとき，リーフ端末は自分の持っている情報を送信したのちには完全に待機状態になる．つまり，明らかにリーフ端末の周りでは観測できるメッセージ量が少なくなり，攻撃者にリーフ端末であるということを推測される恐れがある．そこで，リーフ端末は自分の情報を送った後，複数回ダミーのメッセージを送信するという手法をとる．このメッセージの送受信者情報を含むすべての内容は完全に乱数で生成する．送信端末の親がそのメッセージを受信した場合，自分の持つ鍵で復号を試みても意味のある情報とならないため，親はそのメッセージを破棄する．つまり通信にはまったく影響を及ぼさない．しかも，攻撃者から見てもどの端末がリーフなのかを判断することができない．ネットワークに流れているメッセージがダミーなのかどうかを判断できないためである．これにより，木構造のトポロジを構築するようなネットワークに限定すれば，振舞い解析へのリンク不能性を得ることができる．

5.3 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，保持しなければなら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うえ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．

トポロジ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 2** 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，ルート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，自身のすべ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 2 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ヘッドは発生しない．

5.4 シミュレーション

前節では経路木として完全二分木を想定したうえで，解析的に各プロトコルの比較を行った．本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状況下で行う．シミュレーションで使用した各パラメータを以下に示す．Channel Type は Channel/WirelessChannnel とした．Radio-propagation は Propagation/TwoRayGround とした．Network Interface は Phy/WirelessPhy とした．MAC は 802.11 とした．Interface Queue は Queue/DropTail/PriQueue とした Link Layer は LL とした．Antenna Type は Antenna/OmniAntenna とした．Queue Size は 100 とした．通信範囲は 150 m とした．これらは多数ある先行研究におけるシミュレーションを参考に決定した [8], [9], [10]．

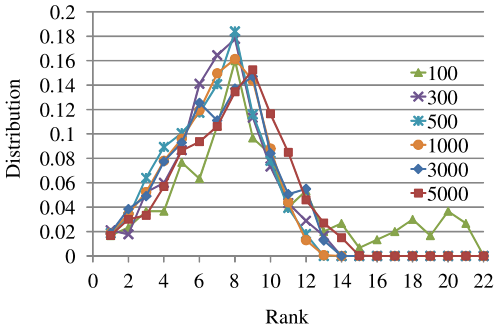

図 1 Rank の分布
Fig. 1 Distribution of rank.

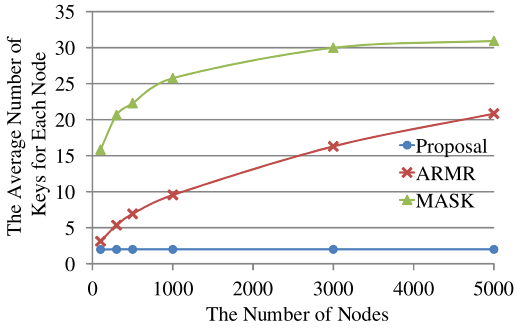

図 2 各端末の平均鍵保有数
Fig. 2 The average number of keys for each node.

5.4.1 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，今回のシミュレーションでは各端末の通信範囲を 150 m と固定しているため，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．しかしそのためには，シミュレーションに先立って，適切な端末密度を決定しなければならない．そこで，まずはシミュレーションの際に用いる端末密度を決定する．そのために，ネットワークエリアを 1 km 四方に固定したうえで端末数を変化させ，RPL を用いて経路制御を行った．ただし，これらのルート端末を原点に固定し，それ以外の端末をランダムに配置するという実験を，各端末数で 3 度行って得られた結果の平均値である．

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** に示す．縦軸は横軸に示した Rank が全端末中に占める割合を示している．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，ランダム配置によるネットワークの構造のばらつきが大きいためである．よって 100/km^2 という端末密度は，ネットワークの構造が不安定になるため不適切である．一方，端末数が 3,000 以上の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である．よって 3,000/km^2 以上の端末密度でも，ネットワークの構造が不安定になるため不適切である．図 1 において，端末数が 300 から 1,000 の場合はグラフの構造が似通っている．特に 500 の場合と 1,000 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，端末密度としては 500/km^2 から 1,000/km^2 の範囲が最も適切な値である．このとき，下限である端末密度 500/km^2 は，最小端末数でネットワークエリアを十分にカバーできる．

以上のことから，1 km 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．

5.4.2 各端末の平均鍵保有数

前項で得られた端末密度を用いて，端末数を 100 から 5,000 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から求める．今回もルートにあたる端末を原点に固定してその他の端末をランダムに配置するという実験を 3 度行ったうえで，得られた結果の平均値を用いて考察を行う．

各端末の平均鍵保有数を**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ほど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，提案方式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．

5.4.3 経路構築の実行時間

経路構築の実行時間を議論する前に，べき剰余演算の実行時間について考察する．これは既存方式，提案方式のどちらの場合においても，べき剰余演算の実行時間が経路構築の実行時間におけるボトルネックになるためである．その考察のため，我々はまず 1,024 bit の大きな素数 p と，その原始根として最小な値 g を定める．また，2 つの自然数の組 (a, b) を用意する．そのうえで，Diffie-Hellman の鍵共有方式において交換用の値となる数の組（$A = g^a \bmod p$，$B = g^b \bmod p$）を求める．また，$K = B^a \bmod p = A^b \bmod p$ となることを確認する．以上，のべ 4 回のべき剰余演算を実行したときの所要時間を 4 で割ることで，1 回のべき乗演算にかかる時間を推定する．

我々の研究室内の機器で実験を行った結果を**表 3** と**図 3**

表 3 鍵共有の実行時間
Table 3 The runtime of Diffie-Hellman key exchange.

Frequency	Memory	Runtime
1.1 GHz	512 MB	1.068 sec
1.6 GHz	512 MB	0.540 sec
2.0 GHz	2 GB	0.329 sec
2.8 GHz	4 GB	0.206 sec

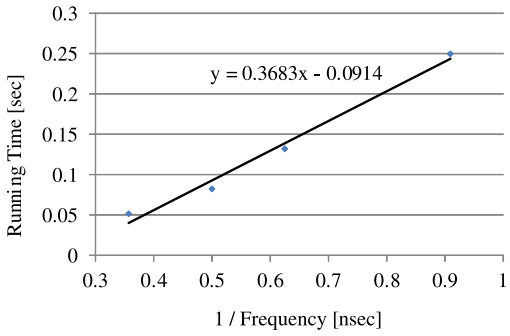

図 3 鍵共有の実行時間
Fig. 3 The runtime of Diffie-Hellman key exchange.

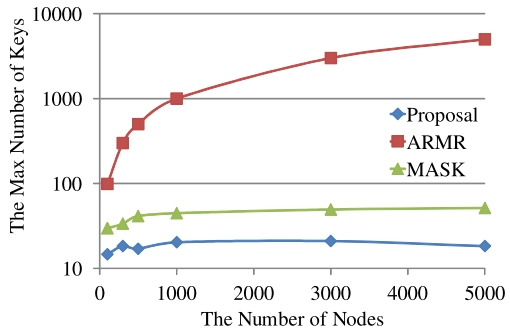

図 4 最大鍵保有数
Fig. 4 The max number of keys for one node.

に示す．市場の動向から，我々はセンサの計算性能として 275 MHz のクロック周波数を想定した．このとき，センサ上でのべき剰余演算の実行時間は 1 回あたり 1.38 秒であると推測することができる．ここで，我々の経路構築の実行時間における実行時間のボトルネックがべき剰余演算にあるという仮定から，経路構築の実行時間 T は以下にあげる N と t から Nt と近似できる．N はそのネットワークにおける最大鍵保有数であり，t は 1 回のべき剰余演算にかかる時間である．

1 つの端末における最大鍵保有数を図 4 に示す．ARMR では最大鍵保有数を示すのはルート端末である．これはすべての端末との経路を構築する際に，それぞれ異なる鍵を生成するためである．つまり自分以外の端末の数だけ鍵を保持しなければならないということである．そのため ARMR ではネットワークの規模が大きくなればなるほど鍵の数が増えるということが分かる．一方，提案方式と MASK では端末 1 台あたりの鍵の数が端末密度に依存する．そのため図 4 が示すように，最大鍵数は今回の実験環境ではほぼ同じような値を示している．

表 4 経路構築の実行時間
Table 4 The runtime of anonymous route establishment.

n	Our Protocol	ARMR	MASK
100	20.24 sec	136.6 sec	40.94 sec
300	25.30 sec	412.6 sec	46.46 sec
500	23.46 sec	688.6 sec	57.04 sec
1,000	28.06 sec	1,379 sec	64.64 sec
3,000	28.98 sec	4,139 sec	67.08 sec
5,000	25.30 sec	6,899 sec	70.84 sec

実際に経路構築の実行時間を計算した結果を表 4 に示す．ARMR では端末の増加による経路構築時間の増加が著しい．端末数が 5,000 台である場合，経路構築に 2 時間程度かかる計算となった．一方，先に示したとおり提案方式と MASK は端末 1 台あたりの鍵の数が端末密度に依存する．提案方式では 27 秒程度，MASK では 75 秒程度で，ネットワークの規模に依存せず経路を構築することが可能であるという結果となった．これらの結果から，我々の提案方式が非常に効率的に経路の構築を行うことが可能であるということを示すことができた．

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ネットワークにおける匿名通信方式のプロトコルを提案し，シミュレーションを行った．その結果，本提案方式は既存方式である ARMR および MASK と比較して，経路を保持する際に必要な記憶容量を抑えることができるとともに，経路構築までの実行時間を小さくできることが明らかになった．また，本提案方式では，端末の鍵数が端末密度に依存するが，最大鍵保有数は端末数に関係なくほぼ同じ値となった．これらのことから，本提案方式は，スマートメータのような大規模な多対一通信環境における匿名通信において有用である．

今後の課題としては，今回の提案方式よりもより安全で匿名性の高い方式を提案することがあげられる．現時点ではネットワーク内部からの攻撃については議論しておらず，特に中間者攻撃などへの対策を含む改善の必要がある．また，現時点ではメッセージ解析攻撃への対策手法として毎回鍵を更新するという方式を取っているが，この方式では特定のタイミング以外で緊急な通信を行うような場合に対応できない．よって，より柔軟な通信要求に対しても対応できるメッセージ解析攻撃への対策も考えなければならない．さらに，通信遅延やパケットロス率など，経路構築時間以外のパフォーマンスの比較や，今回示さなかった他の既存の匿名通信プロトコルとの特性の違いに関する考察などを行うことも考えていきたい．

参考文献

[1] Rathod, V. and Mehta, M.: Security in Wireless Sensor Network: A survey, *Ganpat University Journal of Engineering and Technology*, Vol.1, No.1, pp.35–44 (2011).

[2] Varghese, S.S. and Raja, J.I.J.: A Survey on Anonymous Routing Protocols in MANET, *Proc. 12th International Conference on Networking, VLSI and Signal Processing*, pp.88–92 (2010).

[3] Jeonggil, K., 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, No.4, pp.96–101 (2011).

[4] Zhang, Y., Liu, W., Lou, W. and Fang, Y.: MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks, *IEEE Trans. Wireless Communications*, Vol.5, No.9, pp.2376–2385 (2006).

[5] Dong, Y., Chim, T.W., Li, V.O.K., Yiu, S.M. and Hui, C.K.: ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks, *Ad Hoc Networks*, Vol.7, pp.1536–1550 (2009).

[6] Pfitzmann, A. and Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version v0.34), A Consolidated Proposal for Terminology, Tech. Rep. (2010).

[7] Chen, J.T. et al.: Improving the efficiency of anonymous routing in MANETs, *Computer Communications* (2011).

[8] Clausen, T. and Herberg, U.: Multipoint-to-Point and Broadcast in RPL, *Proc. Network-Based Information Systems*, pp.493–498 (2010).

[9] Liu, J., Kong, J., Hong, X. and Gerla, M.: Performance Evaluation of Anonymous Routing Protocols in MANETs, *IEEE Wireless Communications and Networking Conference* (2006).

[10] Song, R. and Korba, L.: A robust anonymous ad hoc on-demand routing, *Proc. Military Communications Conference* (*MILCOM*) (2009).

中村 彰吾

昭和 62 年生．平成 22 年九州大学工学部電気情報工学科卒業．平成 24 年九州大学大学院システム情報科学府情報学専攻修士課程修了．同年三菱電機情報ネットワーク株式会社入社．修士（工学）．

堀 良彰 （正会員）

昭和 44 年生．平成 4 年九州工業大学情報工学部電子情報工学科卒業．平成 6 年九州工業大学大学院情報工学研究科情報システム専攻修士課程修了．平成 6 年九州芸術工科大学助手．博士（情報工学）．平成 16 年より九州大学大学院システム情報科学研究院助教授（現，准教授）．平成 17 年より 18 年にかけてカリフォルニア大学アーバイン校計算機科学部訪問研究員．情報ネットワーク，ネットワークセキュリティ，コンピュータシステムセキュリティ等の研究に従事．電子情報通信学会，IEEE，ACM 各会員．

櫻井 幸一 （正会員）

昭和 38 年生．昭和 61 年九州大学理学部数学科卒業．昭和 63 年九州大学大学院工学研究科応用物理専攻修士課程修了．昭和 63 年三菱電機株式会社入社後，情報電子研究所（現，情報総合研究所）にて，暗号と情報セキュリティの研究開発に従事．博士（工学）．平成 6 年より九州大学工学部情報工学科助教授．平成 9 年より 10 年にかけて米国コロンビア大学計算機科学科訪問研究員．現在，九州大学大学院システム情報科学研究院教授．平成 16 年より財団法人九州システム情報技術研究所第 2 研究室長（現，財団法人九州先端科学技術研究所情報セキュリティ研究室長）．電子情報通信学会，日本数学会，ACM，IEEE 各会員．