Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

ネットワークアドレスのリンク不能性を実現するセンサーネットワークにおける匿名通信方式

中村彰吾[†1]　岩村恵市[†2]
堀良彰[†1]　櫻井幸一[†1]

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方式を提案する．また，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，効率性と安全性を持つことを，既存方式と比較することで示す．

Anonymous Routing Protocol with Unlinkability of Network Address for Sensor Networks

Shogo Nakamura,[†1] Keiichi Iwamura,[†2]
Yoshiaki Hori[†1] and Kouichi Sakurai[†1]

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. So we propose a new efficient anonymous routing protocol for such multipoint-to-point sensor networks. Moreover, we evidence that our proposal has more efficiency and security than existing ones by comparison.

†1 九州大学大学院システム情報科学府
Department of Informatics, Kyushu University
†2 東京理科大学工学部第 1 部電気工学科
Department of Electrical Engineering, Tokyo University of Science

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[1)] 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通信方式がある．

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，センサー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ー構造を持ち，根に当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，常に根との通信を行うことだけを想定すれば良い．

そこで我々は，多対一通信を行う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．本方式を用いることで，既存の匿名通信方式よりも少ない鍵の共有によって匿名通信を実現することが可能となった．これにより，ユニキャスト通信を全く用いることなく，かつ各端末が保持すべき情報量を従来方式よりも削減できた．さらに，本方式のプライバシー保護性能を強化するために，ネットワークアドレスのリンク不能性を実現するような改良を施した．本稿では，提案方式と既存の匿名通信方式とを比較することで，提案方式が効率性と安全性の面での優位性を持つことを示す．また，提案方式を用いた匿名化を行った際の消費電力の増分についても考察する．

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

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

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] 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 (ルート端末) 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．

RPL の動作は大まかには経路要求フェーズ，経路構築フェーズに分かれており，それぞれ送受信するメッセージの内容が異なる．

経路要求フェーズでは，ネットワークに参加していない端末がそのネットワーク内の端末に向けて DIS と呼ばれる経路要求メッセージを送信する．DIS を受け取った端末は自身の親へその DIS を転送する．ここでの親とは，木において自身とつながっている，自身より 1 つ根に近い端末のことを指す．よって各端末が自身の親に向けて DIS を転送し続けることで，最終的に DIS をそのネットワークのルート端末に到達させることができる．なお，RPL ではルート端末ごとにグラフ ID が定義されており，経路の区別はその ID を用いて行う．このグラフ ID とはルート端末が発行する ID のことであり，各ネットワークを有向非巡回グラフと考えている．一般的な表現としては経路 ID と言い換えることができる．送信先候補となる端末はそれぞれ 1 つのグラフを持っているため，このグラフ ID はルート端末，つまり送信先端末を識別する情報となる．

DIS がルート端末に到達すると経路構築フェーズに入り，ルート端末は DIO と呼ばれる経路構築メッセージをブロードキャストする．DIO を受信した端末はその DIO の送信者を親として設定し，DIO をブロードキャストする．このとき複数の DIO を受信した端末は，あらかじめネットワーク内で定めてある特定の評価指標 (ホップ回数，送信電界強度など) に基づいて，どの端末を自分の親とするか選択する．各端末はこの評価指標に基づいて Rank を設定する．今回はホップ回数を評価指標として考察を行う．この Rank は DIO に付記されており，本稿では転送されるごとにインクリメントされるとする．こうすることで，ルート端末まで最も少ないホップ回数で通信を行うことができる経路を構築することが可能となる．複数の DIO が到達した際には，到達した DIO に含まれている Rank の値が小さいほうを親端末として選択すればよい．

この DIO に含まれる可変情報は以下の 3 つである．

- DIO のバージョン数
- 送信端末の Rank
- グラフ ID

また，経路情報として各端末は以下のものを保持する．

- グラフ ID
- 自身の Rank
- 自身の親端末のアドレス
- DIO のバージョン数

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．ただしこのグラフは必要におぷ時手更新されるものであるため．

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．

一般的に言われる暗号化通信との違いは，特に送受信者に関する情報に対して暗号化を行うかどうかという点にある．通常の暗号化通信はメッセージの本文を暗号化するだけであるのに対し，匿名通信では送受信者の情報も暗号化を行う．

なお，一般に匿名通信と呼ばれるものは，端末間でやり取りする全てのメッセージの送受信者情報を秘匿して行う通信のことを指す．そのため，経路制御に用いるメッセージにも匿名化を施すようにすることが望ましく，ゆえに匿名通信プロトコルには経路制御の機能も持ち合わせているものが多い．

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

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)[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．

3.3 先行研究[6)]

我々はこれまでに，多対一通信を行うセンサーネットワークのための匿名通信プロトコルを提案している．このプロトコルは，特定の終点に向けてエリア内のすべての端末がメッセージを送信するという仮定の下で，既存方式よりも効率的にルーティングおよび匿名化を行うことができる．その特徴として，経路要求メッセージをワンタイムキーで暗号化し，経路構築メッセージには特定の端末の ID やネットワークアドレスなどを含ませず，ブロードキャストによる通信のみでメッセージのやり取りを行う，という点が挙げられる．

3.4 各プロトコルの評価

3.4.1 攻撃者モデル

各プロトコルの評価に先立って，本稿に置いて想定されている攻撃者のモデルを定義する．本稿で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．攻撃者はセンサー端末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，解析することができるものとする．なお，攻撃者がネットワーク内に入ってトラフィック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．

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	√	√	√
ネットワークアドレスのリンク不能性		√	√
振る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	√	√	√

3.4.2 匿名性の比較

表 1 は我々の先行研究での提案方式と既存方式とで匿名性を比較したものである．匿名性の評価を行う上で必要な要件に関しては既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った[7)8)]．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走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ー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，ふるまい解析の 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 に示すよう

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

に，我々の提案方式においてはネットワークアドレスのリンク不能性と振る舞いのリンク不能性が欠如しているという問題点がある．

ネットワークアドレスのリンク不能性とは，トラフィックに対して内容解析攻撃を行われた際の，送受信者のネットワークアドレスに対してリンク不能性のことを指す．ここでの内容解析攻撃とは，同一の送受信者アドレスを持つ複数のトラフィックに対して，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，一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，送受信者に関するフィールドは全く同じ暗号文になってしまう．そのため，そのようなトラフィック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置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ーとして木構造を構築するため，その方針を取ることができない．

また，振る舞いのリンク不能性とは，トラフィックに対して振る舞い解析攻撃を行われた際の，トラフィック間のリンク不能性のことを指す．ここでの振る舞い解析攻撃とは，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ーを構築するため，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トラフィック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トラフィック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，リーフ端末は逆に一切の中継を行うことがない．そのため，攻撃者から見て最もトラフィックのやり取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，振る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ーに特有の問題であると考えられる．

以上のように，これまでの我々の提案方式には 2 つの問題点が残されていた．そこで本稿では，これらの問題点のうち，ネットワークアドレスのリンク不能性の不足を補う，多対一通信を行うセンサーネットワークにおける匿名通信方式を改めて提案する．なお，本稿では上記 2 点以外の特性についての説明および評価は割愛する．

4. 提 案 方 式

今回の匿名通信方式への要件は以下のようなものとなる．

- 大枠は過去に我々が提案した方式を用いる．
  - メッセージの暗号化には共通鍵暗号方式を用いる．
  - リアクティブな経路制御を行う．
  - 各リンクで鍵を共有する．
- ネットワークアドレスのリンク不能性を持つ．

4.1 ネットワークアドレスのリンク不能性の実現

今回想定してい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．

- 同一の送受信者からのトラフィック内には常に共通する情報が存在する．
- 異なる送受信者からのトラフィック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良い．

- 送受信者が同一のトラフィックであっても共通する情報が含まれないようにする．
  - 毎回の通信時に使用する鍵を変更する．（鍵更新方式）
  - 常に各端末のネットワークアドレスに関するフィールドを変化させる．（アドレス更新方式）
- 全ての送受信者からのトラフィックを同一の内容にする．

このうち，全ての送受信者からのトラフィックを同一の内容にするという方式は，実際問題として不可能である．そのため，送受信者が同一のトラフィックであっても共通する情報が含まれないようにするという方式に焦点を絞って検討する．

4.1.1 鍵更新方式

ます，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ーを想定する．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上で必須となるアプリケーションの一つである．スマートメーター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することにより，送受信者情報を暗号化した結果が毎回異なるものとすること

ができる．これにより，スマートメーター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．

4.1.2 アドレス更新方式

次に，常に各端末のネットワークアドレスに関するフィールドを変化させるという方式を検討する．これは，ネットワークアドレスとして処理する部分に乱数を付随させ，その乱数ごと暗号化および復号化をすることで実現できる．例えば通常の IP アドレスであれば 32bit の値を持っているため，ネットワークアドレスとしてこの 32bit の値を暗号化するのではなく，32bit の乱数を連結させた 64bit の値を暗号化して処理する．トラフィックを受信して復号化を行った時には，乱数部分のフィールドを無視して元のアドレス部分を取り出し，それに再度別の乱数を連結させて暗号化し，処理すれば良い．

この方式は鍵更新方式と異なり，任意のタイミングでの通信に適用できる．また，リンク不能性を得るために通信をする必要がないという利点もある．しかも乱数の生成は鍵更新方式でも行っているため，アドレス更新方式のほうが鍵更新方式よりも確実に効率的な改善手法であることが分かる．

4.2 提案における前提

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共通の宛先となる．以下，この端末のことを RPL と同様にルート端末と呼ぶ．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．そして，全ての端末はあるハッシュ関数 H を共有しているとする．また，2 つの値 (g, p) 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の Diffie-Hellman 鍵共有を行う際に使用される．さらに，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る．最後に，各端末はネットワークアドレスと同 bit の乱数を生成することができるとする．以下では始点端末 S からあるルート端末 D にむけて経路を構築し通信を試みると仮定する．

4.3 匿名経路要求

まず，S は乱数 r を生成する．そして，S のネットワークアドレス IP_S に r を連結した I_S，D のネットワークアドレス I_D に同じく r を連結した I_D およびワンタイムキー O を，D の公開鍵 K_D によって暗号化する．さらに，r のハッシュ値 $H(r)$ を求める．その上，S は r を O で暗号化した $O(r)$ を得る．

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 $K_D(I_S)$，$K_D(I_D)$，$K_D(O)$，$H(r)$ および $O(r)$ 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 $K_D(I_S)$，$K_D(I_D)$ および $K_D(O)$ を自身の秘密鍵で復号する．I_D の前半 bit が IP_D 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 I_D の後半 bit のハッシュ値を改めて計算し，$H(r)$ と比較する．2 つの値が等しければ，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 IP_S と IP_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．

4.4 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 IDI_G，グラフシーケンスナンバー N_G，送信端末の Rank 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．

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共有する鍵を生成する．具体的には，自身の x と RREP 内の RREP 内の y から親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 Rank 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．この処理により，自身の子にあたる端末，つまり自身の Rank よりも 1 だけ大きな RREP を受信した際には，自身の x と RREP 内の y から子端末と共有する鍵を生成する．

この繰り返しにより，全ての端末は I_G，N_G，自身の Rank，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 IP_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，IP_S を知ることもできない．さらに，万一経路表が漏れたとしても，経路表内に親端末および子端末のネットワークアドレスは含まれていない．よってこのフェーズにおける匿名性も満たされている．

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

4.5 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．このとき，ネットワークアドレスに関するフィールド (IP_S, IP_D) には，新たに生成した乱数 r' を連結した I'_S および I'_D を用いる．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．その際，K_C によって得られたネットワークアドレスのフィールド (I_S, I_D) については，後半 bit を別の乱数 r'' に置き換えて暗号化する．

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．

5. 評　　価

本稿では効率性の評価として，消費電力に関する検討を行う．比較対象とするのは，本稿でも取り上げた RPL という経路制御プロトコルである．このプロトコルは前述のとおり，多対一通信に特化した経路制御プロトコルである．本稿では，匿名化を行うことでどの程度消費電力が増大するのかを考察する．

5.1 RPL と提案方式との対比

提案方式は RPL を基に経路制御を行うため，RPL と似た処理を行う部分が多数存在する．そこで消費電力の評価にあたって，まずはそれぞれに共通する箇所と異なる箇所を明確にする必要がある．

5.1.1 共　通　点

RPL と提案方式とで共通する箇所を以下にまとめる．

- 多対一通信を目指す．
- 木構造を持つグラフによって経路を管理する．
- 経路の管理をグラフ単位で行う．
- Rank によって最適な経路を選択する．

これらの特徴から，仮に端末の配置が同じ状況であれば，ネットワークの構造はどちらのプロトコルを用いても同じものになると考えられる．よって，消費電力の比較を行う際には，ネットワーク全体の挙動は考慮する必要がなく，端末単位での動作を比較するだけで良いと考えることができる．

表 2 RPL と提案方式の相違点
Table 2 The Differences between RPL and Our Proposal

	RPL	提案方式
親端末との通信方法	相手のアドレスを指定してユニキャスト	相手との共通鍵で暗号化してブロードキャスト
経路要求時の匿名化	何もしない	暗号化により行う
経路構築用の情報	DIO バージョン数	グラフシーケンスナンバー
	送信者の Rank	送信者の Rank
	グラフ ID	グラフ ID
	送信者アドレス	送信者の鍵共有用パラメータ
経路表内の情報	DIO バージョン数	グラフシーケンスナンバー
	自身の Rank	自身の Rank
	グラフ ID	グラフ ID
	親端末のアドレス	親と共有している送信用鍵
		子と共有している受信用鍵
パケット転送時の処理	パケットには何も処理をしない	パケットを受信用鍵で復号し乱数を置き換えて送信用鍵で暗号化する
パケット内の経路情報	グラフ ID	グラフ ID
	送信者ネットワークアドレス	送信者ネットワークアドレス
		乱数 (上記 2 つに連結)

5.1.2 相　違　点

表 2 は RPL と提案方式で異なる箇所をまとめたものである．これによると，提案方式では端末間通信にユニキャストを用いないためにネットワークアドレスを極力使用する必要がないことが分かる．また，RPL と同様に宛先となるルート端末の識別にネットワークアドレスと一対一で対応されているグラフ ID を用いることで，極力ネットワークアドレスを用いることを避けることができる．その他，経路構築メッセージの内容と経路表の内容に関しては，RPL と提案方式とではほとんど差異がない．

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

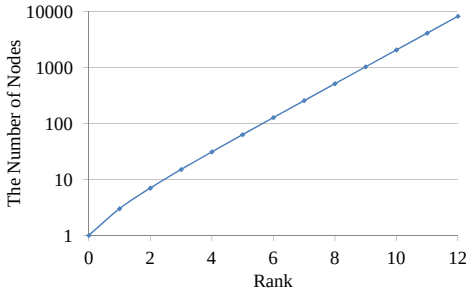

図 1 完全二分木の収容可能端末数
Fig. 1 The Maximum Number of nodes in Complete Binary Tree

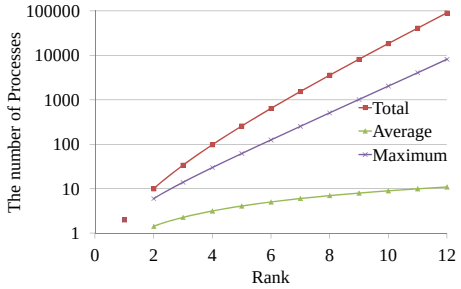

図 2 完全二分木での処理回数
Fig. 2 The Number of Processes in Complete Binary Tree

ただし，提案方式では RPL と違い自分の子に関する情報も経路表に保持しなければならないという特徴がある．このため，ある端末の直下に存在する子の数が多くなるような環境では，記憶容量に対する負荷が大きくなってしまうと考えられる．そのような環境の例として，端末が密集してセンサーの通信範囲内に多数の端末が存在してしまうような環境が想定できる．この場合，匿名化することによって消費電力が増加すると考えることができる．

また，経路構築後にルート端末と各端末が通信を行う場合，RPL であれば中継端末は単に受け取ったパケットをフォワーディングするだけで良いのに対し，提案方式では

(1) 受信したパケットを受信用鍵で復号
(2) 乱数を生成してグラフ ID と送信者ネットワークアドレスに連結
(3) 送信用鍵で暗号化してパケットをフォワーディング

という処理を行う必要がある．これは各端末がパケットを中継するたびに行う処理であるため，ネットワーク全体ではかなりの回数行われる処理であると考えられる．さらに，局所的にみるとルートに近い端末ほどこの処理を多く行う必要がある．仮にネットワークを表す木構造グラフとして，特徴解析を行いやすく段数を抑えることが可能な完全二分木を想定すると，Rank の最大値が n のときネットワーク全体で $\sum_{i=1}^{n} i2^i$ 回の処理を行うことになる．

5.2 消費電力の考察

前節で述べた相違点を基に，提案方式によって匿名化処理を行う場合の消費電力の増分を考察する．ここではセンサーのコントローラーとして，ATmega128L を想定している．また，提案方式での乱数生成のために，ATmega128L とは別に乱数生成器を用意する．

なお，本稿では経路が既に構築された状態を想定し，経路の再構築は起きないものとする．

5.2.1 匿名化処理の回数

図 1 および**図 2** は，トポロジーとして完全二分木を想定したときの，ある Rank において収容できる端末の最大数とそのときの処理回数をグラフ化した図である．ただしここでの処理回数とは，全端末がルート端末に向けて一斉に通信を行った際の処理回数のことを指す．この表から，ネットワーク全体を通してみればそれほど多くの処理が必要となるわけではないと考えることができる．しかしルート端末に近い端末に着目してみると，単に RPL を適用した場合と比べ，膨大な回数の処理を行う必要があることが分かる．この結果を基に，ネットワーク全体の消費電力の増分と端末当たりの平均消費電力の増分を考察し，さらに消費電力が最大でどの程度まで大きくなることを見込む必要があるのかを検討する．

5.2.2 匿名化処理にかかる電力の考察

暗号化方式として AES を利用した場合，一度の暗号化・復号化にかかる電力は，ATmega128L 上で 2.49μJ である[9]．また，40kb/s の乱数生成器[10] を用いれば，32bit の乱数を生成するには 800μ 秒かかるため，1 回の乱数生成にかかる電力は 0.832nJ となる．この乱数生成器と ATmega128L との通信時に発生する消費電力は，福田らの提案した送受信 IC[11] を用いて接続することで 31.36pJ となる．これらの結果から，提案方式での一度のフォワーディングでの消費電力は，RPL と比較して約 5μJ 増加すると考えることができる．

表 3 は，端末数と消費電力の増分についてまとめた表である．これは先の消費電力考察と図 1，図 2 を基に，ネットワークとして完全二分木を想定して全端末がルート端末が一斉に通信を行った場合を想定した結果である．これによると，仮にエリア内の端末数が 5000 個程度であったとしても，最もルート端末に近い端末が一度の一斉通信で負担する電力は

Vol.2012-DPS-150 No.34
Vol.2012-CSEC-56 No.34
2012/3/1

表 3 完全二分木における消費電力の増分
Table 3 The Incremental Power Consumption on the Comprete Binary Tree

端末数	ネットワーク全体の消費電力増分 [J]	平均消費電力増分 [J]	ルート直下端末の消費電力増分 [J]
1	0	0	—
3	10μ	3.33μ	10μ
7	50μ	7.14μ	30μ
15	170μ	11.33μ	70μ
31	490μ	15.81μ	150μ
63	7.69m	20.48μ	310μ
127	17.93m	25.28μ	630μ
255	40.97m	30.16μ	1.27m
511	92.17m	35.09μ	2.55m
1023	204.81m	40.05μ	5.11m
2047	450.57m	45.03μ	10.23m
4095	983.05m	50.02μ	20.47m
8191	2.13	55.01μ	40.95m

50mJ 弱であることが明らかになった.

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ーネットワークにおける匿名通信方式として，これまでの先行研究を改良した方式を提案した．これにより，これまでは得られなかったネットワークアドレスのリンク不能性を得ることが可能となった．また，匿名化を行わない単なる経路制御プロトコルと提案方式を比較し，匿名化のために必要な電力コストの検討を行った．

今後の課題としては，経路構築時の消費電力増分に関しての議論が残っている．本稿では既に経路を構築した状態で，ネットワークの再構築などが発生しないまま通信を行う場合の消費電力の検討しか行っていない．しかし経路構築時には鍵の共有を行う必要があるため，この点における消費電力の増分があると推測できる．また，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．さらに，今回は問題点の提示のみで終わっている，振る舞いのリンク不能性を得るための方法なども検討していく必要がある．

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, *Proceedings of the 12th international conference on Networking, VLSI and signal processing*, pp.88–92 (2010).
3) K., J., A., T., S., D.-H., D.E., C., J.W., H. and P., L.: 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 Transactions on 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 7*, pp.1536–1550 (2009).
6) 中村彰吾，　堀良彰，櫻井幸一：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，コンピュータセキュリティシンポジウム 2011 (2011).
7) 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).
8) Chen, J.T., Boreli, R. and Sivaraman, V.: Improving the efficiency of anonymous routing in MANETs, *Computer Communications* (2011).
9) Ahmad, S., Rizwan, M.R. and Abbas, Q.: Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography, *International Journal of Computer Applications Special Issue on "Mobile Ad-hoc Networks"*, pp.167–172 (2010).
10) Chen, W., Che, W., Yan, N., Tan, X. and Min, H.: Ultra-Low Power Truly Random Number Generator for RFID Tag, *Wireless Personal Communicarions*, Vol.59, No.1, pp.85–94 (2011).
11) Fukuda, K., h Yamashita, Ono, G., Nemoto, R., Suzuki, E., Masuda, N., Takemoto, T., Yuki, F. and Saito, T.: A 12.3-mW 12.5-Gb/s Complete Transceiver in 65-nm CMOS Process, *IEEE Journal of Solod-State Circuits*, Vol.45, pp.2838–2849 (2010).