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

2008－UBI－19（1）
2008/7/17

大規模センサネットワークに適したサーバデータ認証方式

野田 潤† 楫 勇一‡ 中尾 敏康†

†NEC サービスプラットフォーム研究所 〒630-0101 奈良県生駒市高山町 8916-47
‡奈良先端科学技術大学院大学情報科学研究科 〒630-0101 奈良県生駒市高山町 8916-5
E-mail: † {j-noda@cw, t-nakao@bp}.jp.nec.com, ‡ kaji@is.naist.jp

あらまし センサネットワークにおける利用に適した，サーバデータ認証方式を提案する．データ認証は，データの偽造や改変を検知するための仕組みであり，安全で信頼性の高いシステムを構成するための基礎的技術である．一台のサーバが多数のノードを制御するセンサネットワークでは，特にサーバが送信するデータの認証が重要となる．本稿では，ノードの部分集合(グループ)を複数定義し，グループ鍵とメッセージ認証子を利用したサーバデータの認証方式を提案する．単純なデータ認証方式に比べ，提案法では，鍵情報や制御信号などの重要なデータの送受信にかかるデータ認証のオーバヘッドを削減することが可能となる．中規模自治体(約 38,000 世帯)におけるテレメータリング(遠隔検針)をモデルケースに想定し，提案法の効果を定量的に評価したところ，約 1/644 のサーバ送信量の削減が見込めることを確認できた．

キーワード データ認証，メッセージ認証子，センサネットワーク，マルチキャスト，ブロードキャスト

A Scalable Server Data Authentication Scheme for Sensor Networks

Jun NODA† Yuichi KAJI‡ and Toshiyasu NAKAO†

† Service Platform Research Labs., NEC, 8916-47 Takayama-cho, Ikoma-shi, Nara, 630-0101 Japan
‡ Nara Institute of Science and Technology, 8916–5 Takayama-cho, Ikoma-shi, Nara, 630–0192 Japan
E-mail: † {j-noda@cw, t-nakao@bp}.jp.nec.com, ‡ kaji@is.naist.jp

Abstract We propose a new server data authentication scheme for sensor networks. Data authentication is a basic technology to detect spoofing and malicious modification of data, and it is a basic component of a secure network. In a sensor network where one server controls many nodes, it is very important to authenticate the data transmitted by the server. In this paper, we propose a server data authentication scheme that incurs less server communication overhead than a simplistic data authentication scheme. Our proposed scheme leverages structured group keys and message authentication code. Finally, we introduce an example application of our proposed scheme and evaluate its effects quantitatively.

Keyword data authentication, message authentication code, sensor network, multicast, broadcast

1. はじめに

センサネットワークは，センサ機能を有する多数の小型端末(ノード)と，それを管理する計算機(サーバ)から構成されるネットワークの一種であり，防犯，防災，広域計測等，幅広い応用範囲が期待される技術である[1][2]．通常，各ノードは無線通信機能を有しており，収集した情報の送信や，他のノード，サーバからの情報受信は，この無線通信機能を利用することによって行われる．無線通信は傍受が容易であり，また，情報送信エンティティの特定が困難であるという意味で，セキュリティ的には脆弱な通信基盤であるといえる．したがって，センサネットワークに高い安全性や信頼性が要求される場合には，暗号化やデータ認証等の仕組みを実現することが不可欠となる．

本研究では，センサネットワークにおけるデータ認証について議論する．データ認証とは，通信路等を介して受信したデータの偽造や改変を検知するための仕組みであり，通信途中でのデータ改ざんや，悪意を持つ第三者が他人になりすましてデータを送信する行為を抑止するための機能を提供するものである．データ認証は，高いセキュリティが要求されるデジタル通信全般において必要とされる機能であり，汎用コンピュータネットワークでは，電子署名やメッセージ認証子(Message Authentication Code, MAC)を利用することにより実現される[3]．電子署名は，通常，公開鍵暗号に類する技術を利用して実現される．数百から数千ビットの整数演算が必要とされることも多く，計算資源の限定されたノード上でこれを実現することは，あまり現実的でない．一方，MAC は対称鍵暗号ベースの技術であり，それほど大きな計算資源を必要としないとい

う利点がある．したがって，センサネットワークにおけるデータ認証を考える際には，MAC 技術を中心として検討を行うことが有効であると考えられる．

MAC とは，MAC 鍵と呼ばれる秘密情報とデータ(メッセージ)から一意に計算される値である．本稿では，MAC 鍵 k，データ m から定まる MAC を MAC(k,m) と表記する．二人のユーザ A，B は，通信に先立って MAC 鍵 k を事前に共有し，これを秘密に管理しておく．A が B に対してデータ m を送信する際には，データ m に加え，MAC 情報である MAC(k,m)も同時に送信する．受信者 B は，受信したデータと自らが保有する MAC 鍵 k から MAC を再構成し，それが送信されてきた MAC と一致するか否かを検査する．もし両者が一致すれば，受信データは間違いなく A から送られてきたものと認め，一致しなければ，これを不正データとして破棄する．MAC を用いたデータ認証の安全性を確保するためには，MAC 鍵を知らない第三者には MAC(k,m)の計算が困難となるようする必要がある．共通鍵暗号を利用する方式[4]，鍵付きハッシュ関数を用いた方式[5]等，様々な MAC の実現法が検討されているが，本稿では，特定の MAC を対象とせず議論を行うこととする．

MAC の問題点は，三人以上のユーザを含むグループ通信において，簡潔かつ効率的にデータ認証機能を提供することが難しい点にある．たとえば A,B,C の三人のユーザが同一の MAC 鍵を有する場合を考える．このとき，A が B および C に対して MAC 付きデータを送信したとしても，受信者 B(または C)は，当該データが C(または B)によって送信された可能性を否定できない．すなわち，「グループ内の(自分以外の)誰かが送信した情報であることは確認できるが，送信者の特定はできない」という意味で，データ認証機能を十分に提供しているとは言いがたい．この問題を避けるには，A と B の間，B と C の間，C と A の間で相異なる MAC 鍵を準備しておき，たとえば A がデータを送信する際には，B 用の MAC と C 用の MAC の二つの MAC 情報を添付する必要がある．一般には，グループに属するユーザ数に比例した個数の MAC を送信する必要があるという意味で，この方式ではスケーラビリティの確保が困難である．

本研究では，センサネットワークにおいてサーバから送信されるデータの認証を考える．センサネットワークでは，ノードが観測して入手した情報はノードからサーバの方向に流れるが，ネットワークを制御するための情報等は，逆に，サーバからノードの方向に流れることになる．制御情報が改ざんされたり，偽造されたりした場合，ネットワーク全体が不正者の制御下に置かれるおそれもあるため，サーバが送信するデータの認証は非常に重要となる．サーバとノードとの間で一対一通信を行う場合，通常の MAC の使用によって問題を解決することも可能であるが，サーバが複数のノードに対して同報通信的にデータを送信する場合，既に述べたグループ通信における MAC の問題に直面する．

この問題に対処するため，ノードを部分集合に分割し，各部分集合ごとに MAC を与える方式を考える．ただし，一種類の集合分割を考えたのでは，グループ通信における MAC の問題の本質的な解決にはならない．そこで本研究では，ノード集合に対する複数の集合分割を考え，厳密な意味でのサーバデータの認証を実現する．集合分割の与え方には自由度があるが，例えば 3 節で後述するようにノード識別のためのアドレス空間に対応させて分割を定義することが考えられる．

以下，第 2 節では，センサネットワークにおける既存の鍵管理技術について簡単に紹介し，単純な方式ではサーバデータの認証の実現が困難であることを示す．第 3 節にて提案法を与え，第 4 節では，中規模自治体におけるテレメータリング(遠隔検針)を想定した数値評価を与える．

2. 既存の鍵管理技術と単純な方式

情報秘匿，認証等，ネットワークセキュリティの実現にあたって重要となるのが，鍵管理の問題である．通常のコンピュータネットワークでは，公開鍵暗号や鍵共有プロトコル等を利用することによって鍵管理の問題を解決しているが，これら方式では，その内部では非常に規模の大きな演算を行う必要があるため，(利用可能な電力も含めて)計算資源の限定されたセンサノードでこれを実装，利用することは望ましくない．したがって，センサネットワークでは，対称鍵暗号や一方向性ハッシュ関数等，計算負荷の小さな基礎技術のみを利用し，情報の制御を適切に行うことによって，鍵の生成や流通等を安全に実現する必要がある．その際には，設置されたセンサノードを物理的に保護することが難しく，ノードの盗難が切実な問題となる場合もあること，製造コストの関係でノード自体の耐タンパ性が期待できず，ノード内部の情報が漏出する可能性が高いこと等，センサネットワーク特有の条件や制約についても，十分注意する必要がある．

GKMP[6]や LKH[7]は，汎用のネットワーク向けに開発されたグループ鍵管理プロトコルであるが，公開鍵暗号等を利用しないという点で，センサネットワークへの応用も可能な技術である．たとえば文献[8]などに，LKH に類する方式をセンサネットワークに適用した事例をみることができる．これら方式では，ユーザ(ノード)全体で一つのグループを構成し，同一のグル

ープ鍵を全ユーザ(全ノード)が共有することを目標としている．しかし，この目指す枠組みは，ノード盗難の可能性が無視できないセンサネットワークにおいては，適切なものになりえない．センサネットワークでこれら方式を利用する場合，一台のノードが盗難にあっただけで全てのノードの鍵を更新する必要が生じるため，運用コストや通信オーバヘッド等が増大することが予想される．

LEAP[9]は，センサネットワークでの利用を念頭において提案された鍵管理プロトコルである．LEAP では，ノード全体からなるグループだけでなく，一部のノードから構成される部分グループの存在を許容しており，各部分グループについて，グループ鍵の生成・更新が可能となっている．GKMP や LKH に比べてより柔軟でスケーラブルな仕組みとなっているが，各ノードが正確なタイマを内蔵し，決まった時刻に，内部に記録されたマスタ鍵を確実に消去することが要求される．ノードの故障をまったく許さない仕組みとなっているが，大量生産される低コスト機器の動作不良を認めないという意味で，実現可能性がどの程度あるのか，明確で無い一面もある．また，前節で述べたように，グループ鍵はデータ認証用の MAC 鍵として機能しないため，本研究で考えるサーバデータの認証目的には利用できない．

グループ通信におけるデータ認証を意識した研究としては，SPINS[10]が挙げられる．SPINS は，ノード対間の暗号鍵共有プロトコル SNEP と，放送用 MAC 鍵(本稿でいうサーバデータ認証用 MAC 鍵にあたる)の管理プロトコル μ-TESLA とから構成される．μ-TESLA は，いわゆるハッシュ連鎖を利用して MAC 鍵の管理を行うものであり，サーバは，ハッシュ連鎖中に出現する情報を MAC 鍵として利用する．一定時間経過後，MAC 鍵は，ハッシュ連鎖を一段遡ったものに切り替えられ，同時に，サーバはそれまで使っていた古い MAC 鍵を公開する．この時点で各ノードは，過去に受信したデータの認証を行うことが可能となる．この方式では，データの受信から認証までに遅延が生じること，MAC 鍵公開のタイミングで，中継ノードによる不正行為を許してしまう(サーバになりすまし，下流ノードにデータを送信できる)等の問題があり，データ認証を十分に実現しているとは言いがたい．

著者らの知る限り，センサネットワークにおいてサーバデータの認証を可能にする特別な仕組みは提案されていない．原理的には，サーバと各ノードとの間で個別に MAC 鍵を共有しておけば，サーバデータの認証を実現することは可能である．しかし，この場合サーバは，一つの送信データに対して多数の MAC を添付することになり，また，データの中継を行うノードも多量のデータを処理する必要が生じる．この単純な方式からどの程度まで効率を改善できるかが，サーバデータ認証の仕組みを評価する際のポイントとなる．以降ではこの単純な方式を，単純個別鍵方式と呼ぶ．

3. 提案方式

3.1. 方式説明

データ認証技術を元に，複数のノードが効率的にサーバからのデータを認証する方式を提案する．本提案方式では，以下の仮定をおく．まず，各ノードを識別子の階層構造で一意に特定できるものとする．ここで識別子をアドレスと呼び，また各階層におけるアドレスの取り得る範囲をアドレス空間と呼ぶ．図 1に，アドレス空間とアドレスの例を示す．本例では，アドレス空間 1 はアドレス 1-1，1-2，...，1-p を含み，アドレス空間 2 はアドレス 2-1,2-2，...，2-q を含み，アドレス空間 3 はアドレス 3-1,3-2，...，3-r を含む．p,q,r は，各アドレス空間において，全ノードを識別するために必要なアドレスの最大数を示している．図 1では，(1-1,2-q,3-2)で識別されるノード i を例示している．

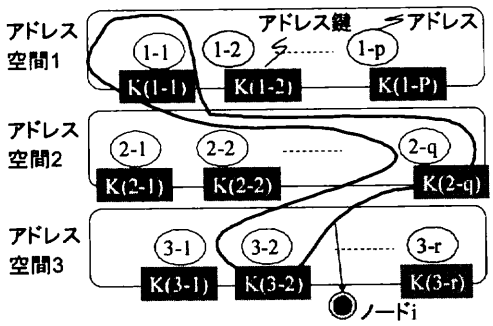

図 1ノードのアドレス空間とアドレス鍵

以上の仮定の下，ノードがサーバからのデータを認証するフローチャートを図 2に示す．N(≧1)台のノードが一斉にサーバからのデータを認証する場合を想定できるが，図 2では代表してノード i(1≦i≦N)のフローを示している．

最初に，サーバからのデータ認証処理を開始する前の準備について説明する．まず，サーバは，認証に先立つ段階において，N 台のノードを複数のアドレス空間のアドレスの組合せによって，一意に識別する(S1)．

次に，サーバは，ノード識別のための各アドレス空間のアドレス adr に，ユニークな秘密情報(アドレス鍵)K(adr)を対応付ける(図 1)．そして，サーバは，各アドレス空間についてアドレスが一致するノードの集合(ノードグループ)に対して，同じアドレス鍵を安全な方法を用いて割り当てる(S2)．

次に，サーバからアドレス鍵を割り当てられたN台のノードは，割り当てられたアドレス鍵を秘密情報として記憶する(C1)．また，サーバは，各ノードに対して割り当てた全てのアドレス鍵を記憶する(S3)．以上のステップの完了により，ノードは，サーバからのデータを認証するステップに進むことが可能となる．

上記のステップ完了後，サーバがN台のノードに対してメッセージを一斉送信する場合等に，N台のノードが，同時にそのメッセージが正規のサーバからであるか否かを認証したい状況が発生したとする．この場合，サーバは，ノード識別のための各アドレス空間についてアドレスが一致するノードグループに対して，アドレスに対応させたアドレス鍵を用いてMACを生成する(S4)．そして，サーバは，生成したMACを，当該ノードグループに対して一斉配信する(S5)．この場合，サーバは，MACの一斉配信の方法として，マルチキャスト又はブロードキャストによる方法を用いることができる．

サーバは，N台のノードに割り当てた全てのアドレス鍵を用いてMACを生成し，一斉配信が完了するまで，S4,S5の処理を繰り返し実行する(S6)．

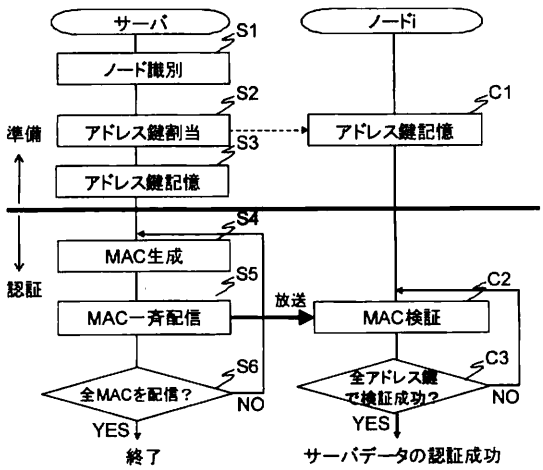

図 2データ認証におけるフローチャート

具体的には，図 1に示す例では，サーバは，アドレス空間 a(1≦a≦3)において，アドレス a-b(1≦b≦アドレス空間 aのアドレス数(p,q又はr))をもつノードグループには，アドレス鍵 K(a-b)を用いて生成した MACを一斉配信する．図 1に示す(1-1,2-q,3-2)のアドレスの組で識別されるノード i は，アドレス 1-1，アドレス 2-q，及びアドレス 3-2をもつ3つのノードグループに属する．そのため，ノード i は，結果的に以下に示す各 MAC(及び任意のメッセージ req_cmd)を受信する．

MAC(K(1-1), req_cmd)
MAC(K(2-q), req_cmd)
MAC(K(3-2), req_cmd)

次に，MACを受信したノードは，MACを自身が記憶するアドレス鍵を用いて検証する(C2)．そして，ノードは割り当てられたアドレス鍵を余すことなく用いて，サーバからの MACを正しく検証できたら，正規のサーバから送られたデータであると判定し，認証を完了する(C3)．一方，ノードが，自身に割り当てられた複数のアドレス鍵のうち，1つでもMACを検証できなかったアドレス鍵がある場合には，認証は未完了であると判断する．

3.2. 考察

本提案方式の適用により，サーバは，単純個別鍵方式によりデータ認証を各ノードに繰り返して適用する(ノード個々にMACを送信する)のではなく，ノード識別のための各アドレス空間で同じアドレスをもつノードグループに対してMACを送信する．

例えば図 1のようにアドレス数が各 p,q,r(≧1)のアドレス数からなる3つのアドレス空間を用いてノードを識別するとき，本提案方式の適用により，送信データ量を削減できる条件を定量的に示す．図 1では階層的にp個のアドレス1つにつきq個のアドレス，このq個のアドレス1つにつきr個のアドレスを指定してノードを識別するので，ノード数は最大 p*q*r 個存在することが可能である．p*q*r 個のノードが存在するとき，単純個別鍵方式に基づき送信される MACの数はノード数と等しいので p*q*r 個となる．一方，本提案方式によって送信される MACは p+q+r 個となる．従って，式(1)が成立するとき，送信するデータ量を削減できることになる．

$$p+q+r < p \times q \times r$$

$$\therefore r > \frac{p+q}{(p \times q - 1)} \quad (p,q,r \geq 1)$$

・・・式 (1)

式(1)が成立する領域(有効領域)を図 3に示す．直感的には p,q,r≧1 でかつ r=(p+q)/(p*q-1)でプロットされる曲面よりも上方にプロット可能な p,q,r のとき，式(1)は満たされるので，本提案方式によって送信するデータ量を削減できることになる．例えば，p≧2,q≧2,r≧2の場合は有効領域に含まれる．一方，p=2,q=1,r=2 の場合は含まれないため，本提案方式は有効でない．

提案方式が想定するネットワークはノード数規模

が大きい大規模なネットワークであり，以上の結果から大規模ネットワーク環境下においては本提案方式が有効に作用すると考えられる．

さらに，サーバとノード対毎に鍵を共有するのではなく，サーバは，ノード識別のための各アドレス空間で同じアドレスをもつノードのグループとの間で鍵を共有する．そのように構成されていることによって，サーバとノード対毎にアドレス鍵を管理する必要をなくすことができ，サーバ側で管理する鍵の個数を削減できる．

また，提案方式は，SPINS よりも運用上の制約が少なく，より現実的に実現可能な方式となっていると考えられる．

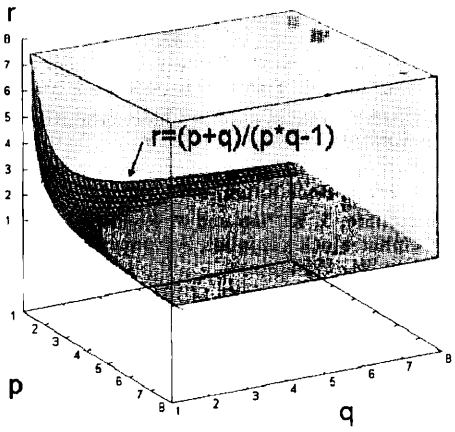

図 3提案方式の有効領域(網掛箇所)

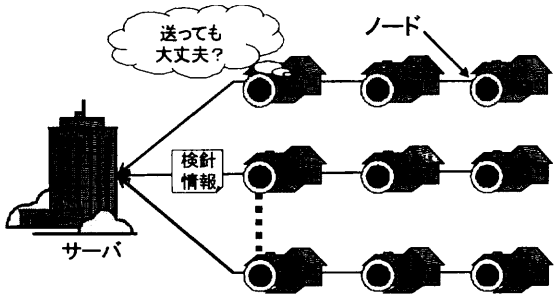

図 4適用例

4. アプリケーションへの適用

センサーネットワークにおける有用なアプリケーションの一つであるテレメータリングへ適用し，実用における通信量削減効果を具体的に評価する．

図 4は，提案方式の適用環境の具体例を示す．本適用例では，複数の世帯からの検針情報を，事業者である検診者に収集する場合を説明する．図 4では，各世帯に検針情報を読み取るノードが設置され，検診者側にネットワークを介して検針情報を収集するサーバが存在する．

図 4に示す例において，各ノードから送信される検針情報は，各世帯のプライバシ情報であり，正規のサーバ以外の第三者に漏洩させることは望ましくない．

従って，サーバが全ノードに検針情報を要求した段階において，ノードグループはデータが正規のサーバからかどうかを認証した後，検針情報を送信する必要がある．本適用例では，一例として，奈良県生駒市の各世帯(約 38000 世帯)に設置されたノードグループによる検針情報の送信時のサーバデータ認証処理について示す．

本適用例では，ノードが設置されている世帯の住所に基づきそれぞれ丁，区，号及び番地に対応するアドレス空間を用いて，ノードの位置を特定する．よって，4 つのアドレス空間上のアドレスをそれぞれ組み合わせると，1 つのノードを識別することができる．また，本適用例では，丁のアドレス空間が p=19 個のアドレスを含み，区のアドレス空間が q=10 個のアドレスを含み，番地のアドレス空間が r=10 個のアドレスを含み，号のアドレス空間が s=20 個のアドレスを含むものとする．従って，本適用例では，p*q*r*s=38000 台のノードが存在するとする．

また，サーバは，各アドレス adr に対して，アドレス鍵 K(adr)を割り当てる．例えば，(区 h，丁 i，番地 j，号 k)で識別可能なノードに対して，K(区 h)，K(丁 i)，K(番地 j)及び K(号 k)の計 4 つのアドレス鍵を割り当て所有させる．サーバは，全てのノードに対して割り当てた全アドレスの総数分のアドレス鍵を保有する．

以上が滞り無く実行されることにより，各世帯のノードは，事業者である検診者側に設置されたサーバからのデータを認証することが可能となる．

アドレス鍵を各ノードに保有させた後，検針情報を収集する場合には，サーバは，全ノードに対して，情報送信要求を行う．この場合，全ノードがサーバからのデータを認証するときの動作は，以下に示す通りとなる．

まず，サーバは，全ノードに対して，検針情報の送信要求 req_cmd を一斉配信する．この場合，サーバは記憶する各アドレス鍵に基づいて MAC を生成し，生

成したMACを放送する．

具体的には，サーバは，全てのアドレス空間について各アドレスを共有するノードグループに対して，当該ノードグループで共有するアドレス鍵を用いて，MACを作成する．そして，サーバは生成したMACを，当該ノードグループにマルチキャスト等の手段を用いて放送する．

各ノードがもつ全アドレスに対応するMACを全て生成可能であるのは，アドレス鍵の持たせ方から，そのノードとサーバのみである．そのため，ノードは，一斉配信されてくるMACのうち，自身のもつアドレス鍵で生成可能なMACを全て検証できたことを条件に，正規のサーバからの送信要求req_cmdであると確認できる．例えば，(区h，丁i，番地j，号k)で識別可能なノードの場合，以下に示した全てのMAC(及び送信要求を示すメッセージ req_cmd)を受信したときに，正規のサーバからの送信要求req_cmdであることを認証可能である．

MAC(K(区h),req_cmd)
MAC(K(丁i),req_cmd)
MAC(K(番地j),req_cmd)
MAC(K(号k),req_cmd)

本適用例では，サーバは，アドレス毎にMACを生成し，一斉配信するので，サーバからネットワーク内に送信されるMACの数は，全アドレス数p+q+r+s=59である．つまり，サーバからネットワーク内に送信されるデータ量は，MACのサイズを|MAC|と記すと，(p+q+r+s)*|MAC| のようになる．

これに対して，単純個別鍵方式により，ノード毎にMACを生成しユニキャストする方式を用いる場合には，サーバからセンサネットワーク内に送信されるMACの数は，センサネットワーク内の全ノード数と同じp*q*r*s=38000である．つまり，サーバからネットワーク内に送信されるデータ量は，(p*q*r*s)*|MAC|のようになる．

以上のように，本適用例では，ノード毎にMACを生成，送信する単純個別鍵方式と比較して，サーバが送信しなければならないデータ量を(p+q+r+s)*|MAC|/(p*q*r*s)*|MAC|≒1/644 に低減することができる．さらに，サーバで管理すべきMACを生成するための鍵の個数もサーバで生成，送信するMACと同数となるので，サーバ側での鍵管理コストも約1/644に削減することができる．

5. おわりに

センサネットワークに適したサーバデータ認証方式について議論を行った．提案方式をテレメータリングに適用し，通信量の削減効果を定量的に示した．

どのようにアドレスを定義するのが良いかは，応用対象および通信形態等に依存するため，アドレスの設計方法等については今後の研究課題であるが，テレメータリングの例のように，住所のような木構造でノードを管理することができる．また，設置場所の階数や方角，ノードの機能や製造元等の物理的な情報を用いてアドレスを定義することも考えられ，適用可能な環境は幅広いと思われる．今後の研究では，このあたりの運用課題に近い問題についても検討していく必要がある．

謝辞 本研究は，独立行政法人 新エネルギー・産業技術総合開発機構(NEDO)の助成事業「半導体アプリケーションチッププロジェクト」の一環として支援を受けて行われたものです．

文　献

[1] R. H. Katz, Next Century Challenges: Mobile Networking for "Smart Dust", Mobicom'99, 1999.

[2] D. Estrin, Next Century Challenges: Data-Centric Networking, Mobicom'99, 1999.

[3] D.R. Stinson, Cryptography - Theory and Practice, CRC Press, Boca Raton, 1995.

[4] M. Bellare, J. Killian and P. Rogaway, The security of cipher block chaining, Advances in Cryptology - Crypto '94, 1994.

[5] B.S. Kaliski Jr. and M.J.B. Robshaw, Message authentication with MD5, CryptoBytes, 1995.

[6] Harney, H., and C. Muckenhirn, Group Key Management Protocol (GKMP) Architecture, RFC 2094, 1997.

[7] C. K. Wong, M. Gouda and S. S. Lam, Secure Group Communications Using Key Graphs, Proc. of ACM SIGCOMM'98, 1998.

[8] 八百健嗣，小沼良平，福永茂，中井敏久: センサネットワークにおける放送型暗号を用いた鍵更新方式，Technical report of IEICE. ISEC,Vol.106, No.597, pp.65-70, 2007

[9] S. Zhu et al, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, ACM Conference on Computer and Communications Security, pp.62--72, 2003.

[10] A. Perrig et al, SPINS: Security Protocols for Sensor Networks, ACM Journal of Wireless Networks, 8, 5, pp.521-534, 2002.