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

2005－DPS－122（42）
2005－CSEC－28（42）
2005／3／23

センサネットワークにおける高信頼ブロードキャストメッセージ認証方式

八百 健嗣*　松村 靖子*　福永 茂*

概要

センサネットワークにおけるノードは，低コスト化を念頭に置いているため，高い処理能力を有する CPU や耐タンパ性装置を仮定することが一般にはできない．本稿では，このような条件においても動作する高信頼ブロードキャスト認証方式を提案する．提案する方式は，共通鍵暗号系で実現するにもかかわらず，メッセージ認証鍵の漏洩やマルチホップ環境下における不正な中継ノードの存在に対して耐性を持つ．提案方式は，メッセージの信頼ブロードキャスト，サーバ管理下の全てのノードからの偽りのない受信確認，認証鍵の公開，の３つのステップからなる．ZigBee 環境において処理時間を検討したところ，高信頼ブロードキャストにかかる時間の抑制が，方式全体の処理時間の削減に有効であることがわかった．

Reliable broadcast authentication in sensor networks

Taketsugu Yao†　Yasuko Matsumura†　Shigeru Fukunaga†

Abstract

Due to the low-cost nature of sensor network nodes, we cannot generally assume the availability of a high-processing-power CPU and tamper-resistant hardware. In this paper, we propose a reliable broadcast authentication working under the above-mentioned circumstances. The proposed method, although based on symmetric cryptographic primitives, is secure against anyone who knew the message authentication key as well as the malicious router nodes in a multi-hop environment. The proposed method consists of three steps; (1) reliable broadcast of a message, (2) acknowledgments without feigning from all the nodes in the network, and (3) disclosure of the message authentication key. We estimated the implementation time of the proposed method in ZigBee environment, and as a result, we found that suppressing the implementation time of reliable broadcast is effective in reducing the whole implementation time of the proposed method.

1 はじめに

近年，無線通信機能を持つセンサを多数設置して設備の管理や環境の観測などに役立てるセンサネットワークシステムが提案されている．センサネットワークシステムは，システムを管理・制御するサーバと，低コストで構成される膨大な数のセンサノードから構成され，マルチホップ通信形態により情報をやりとりすることを想定する．

現在，我々は，センサノードに搭載するソフトウェアの更新を，無線通信を経由して実現しようとしている．前述のように，センサノードの数は膨大である．例えば，ノードに搭載するソフトウェアにバクが発見された時や，ノードに新たな機能を追加したい時，管理者が１つ１つのノードを回収してソフトウェアの更新を行うのは非常に手間のかかる作業である．よって，サーバが更新データをブロードキャストし，ノードが自身のソフトウェアを更新する技術は，センサネットワークシステムにおいて非常に有効な技術である．

センサノードのソフトウェア更新において考慮すべき問題の１つに，セキュリティ問題がある．攻撃者がサーバになりすまし，不正なコードをネットワークに投入するかもしれない（図１参照）．もしノードが不正なコードを排除できないと，センサネットワークシステムは攻撃者によって乗っ取られてしまう可能性がある．また，ソフトウェア更新データはシステムにとって重要なデータであるため，サーバは配布したデータが確実に全ノードに行き届いたことを確認する必要がある．以上のことから，更新データの配布には次の２つの要件を満たす必要があると考える．

- ノードが受け取ったデータをサーバからの正しいデータであると認証すること
- サーバが発信したデータが正しくノードに届いたことを確認すること

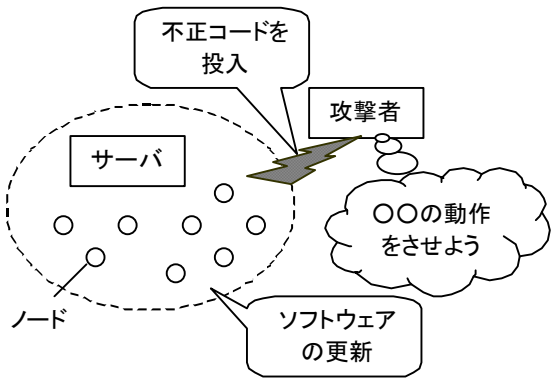


図1：無線通信を用いたソフトウェア更新の脅威

＊ 沖電気工業株式会社 研究開発本部 ユビキタスシステムラボラトリ

†Ubiquitous System Laboratory, Corporate Research and Development Center, Oki Electric Industry Co., Ltd.

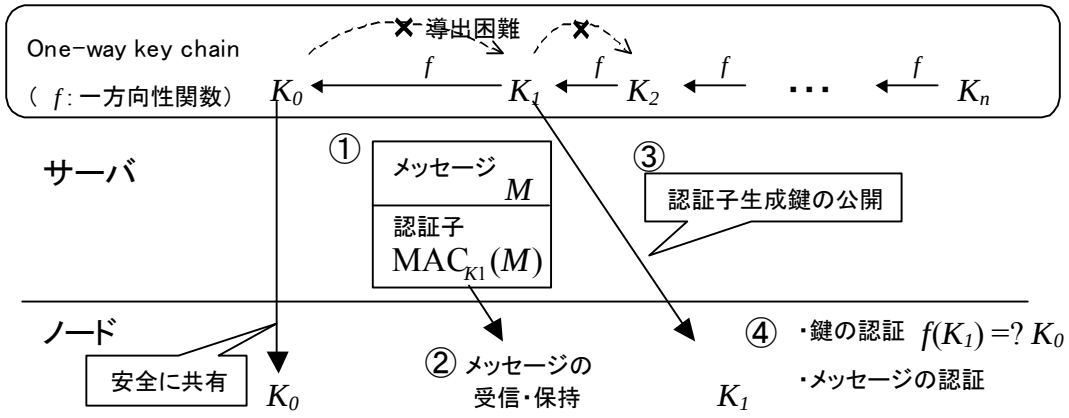


図2: One-way key chainを用いたメッセージ認証の動作例

本稿では，センサネットワークの一般的なネットワーク構造であるマルチホップツリー構造において，上記２つの要件を満たすメッセージ認証方式を提案する．

以下，２章では，ノードのハードウェア面での制約と，起こり得る不正を述べる．３章では，従来方式として One-way key chain を用いたメッセージ認証方式を紹介する．４章では，受信確認を伴った高信頼ブロードキャストメッセージ認証方式を提案する．５章では提案方式の処理時間について考察し，最後にまとめを述べる．

2 ノードのハード制約と起こり得る不正

センサネットワークにおけるノードは，低コストを念頭に置いている．ノードに搭載するＣＰＵは処理能力が低いため，共通鍵暗号のような処理負荷の軽いアルゴリズムを用いて認証する手法が望まれる．また，ノードはコスト高となる耐タンパ性装置を搭載するとは限らない．ノードは小型でモバイル性に富むため，攻撃者がノードを盗難して内部に格納する鍵などの情報を盗み出すかもしれない．

一般的に共通鍵暗号を用いたブロードキャストメッセージ認証は，サーバと全ノードに予め共通の鍵を持たせ，その鍵でメッセージに対する認証子を生成・検証することで実現する．しかし，サーバと全ノードが共通の鍵を持っているため，ノードはサーバを厳密に認証できない．例えば，攻撃者がノードに格納する共通鍵を不正に入手すると，サーバになりすまして不正なデータをノードに認証させることが可能になる．ノードが保持する共通鍵が漏洩しても，サーバへのなりすましに対して耐性があるようなブロードキャストメッセージ認証を実現したい．

3 One-way key chain を用いたメッセージ認証

本章では，従来方式として，ノードが秘密情報を持たずにブロードキャストメッセージを認証できる One-way key chain を用いたメッセージ認証方式について説明する．

3．1 One-way key chain を用いたメッセージ認証の動作と利点

One-way key chain とはランダムな値に一方向性関数を任意回数施して生成した鍵鎖列である．一方向性関数とは，入力値から出力値を求めることは容易だが，出力値から入力値を求めることは困難な性質をもつ関数をいう．One-way key chain を用いたメッセージ認証では， One-way key chain の鍵をメッセージに対する認証子の生成鍵として用いる．

図２を用いて，One-way key chain を用いたメッセージ認証の手順を示す．

＜初期設定＞

サーバと全ノードは共通の一方向性関数 f を共有する．サーバは One-way key chain を生成し，秘密に保持する．ノードは，サーバが生成した One-way key chain の最後の値 K_0 を鍵情報として安全に保持する．

① サーバは，One-way key chain の鍵を生成した順と逆順で使用する．サーバは One-way key chain の次の鍵 K_1（まだノードに公開していない鍵）でメッセージ M に対する認証子を生成し，送信する．

② ノードは，認証子付きのメッセージを受信する．この時点では，受信したメッセージを認証することはできず，メッセージを保持しておく．

③ サーバは，①でメッセージ M の認証子生成に用いた One-way key chain の鍵 K_1 を送信（公開）する．

④ ノードは，受信した（公開された）鍵 K_1 に一方向性関数 f をかけて，予め保持している One-way key chain の鍵 K_0 と一致するかどうかを確かめる．もし一致するならば，受信した鍵 K_1 をサーバが生成した One-way key chain の公開された鍵であると認証し，保持する．次に，鍵 K_1 を用いて②で受信したメッセージ M の認証子を検証する．検証が成功することで，メッセージ M をサーバからの正しいメッセージであると認証する．

この方式の利点は，ノードが秘密情報をもたずにメッセージを認証できることである．ノードが保持する鍵情報は，サーバが次に公開する One-way key

chain の鍵を認証するための情報であり，秘密ではない．もし，攻撃者がノードの保持する鍵情報を不正に入手したとしても，その鍵情報から，次にサーバがメッセージの認証子生成に用いる鍵を求めることは，一方向性関数の原理により困難である．

3．2 マルチホップ通信環境における脅威

前節で説明した方式は，ノードが秘密情報を持たずにサーバからのブロードキャストメッセージを認証できるという利点を持つ．しかし，サーバが公開する鍵情報を先に知るノードが，後に知るノードに対してサーバへなりすますことが可能である．例えば，マルチホップ通信環境におけるルータノードは，伝達遅延をわざと発生させることによりサーバへなりすますことができる．不正なルータノードによるサーバへのなりすましの例を図３に示す．不正なルータノードは，サーバが発信したデータを次ホップのノードへ中継せず，サーバがそのデータの認証子生成鍵を公開するまで待つとする．そして，鍵が公開された時に不正データにその鍵で認証子をつけ，次ホップのノードへ伝達する．後に，既に公開されている認証子生成鍵をまるで今サーバによって公開されたかのように次ホップのノードへ伝達することで，中継先の全ノードに対して不正なデータを認証させることが可能になる．

4 高信頼ブロードキャストメッセージ認証

本章では，マルチホップ通信環境においても，攻撃者がサーバになりすますことが困難で，かつ，受信確認を伴った高信頼ブロードキャストメッセージ認証方式を提案する．

4．1 提案方式の概念

３．２節で述べたように，マルチホップ通信環境では，攻撃者が，公開される鍵情報をノードよりも先に知ってしまう機会が存在する．よって，認証子生成鍵は，サーバが公開した時点で無効であることが望ましい．

提案方式の要点は以下の２つである．

- サーバは，認証させたいメッセージが全ノードに届いたことを確認した後で，メッセージの認証子生成に用いた鍵を公開する．
- One-way key chain の各鍵で認証するメッセージ数を既定し，サーバとノード間で認証の回数同期を行う．

提案方式において，攻撃者が不正データをノードに認証させることができるかどうかは，メッセージの受信確認情報を偽れるかどうかに依存する．

次節では，セキュアな受信確認を実現する一例として，マルチホップツリー構造においてメッセージの受信確認を効率良くかつセキュアに収集する方式について紹介する．

4．2 マルチホップツリー構造に適したセキュアな受信確認方式

本節では，センサネットワークの一般的なネットワーク構造であるマルチホップツリー構造において，

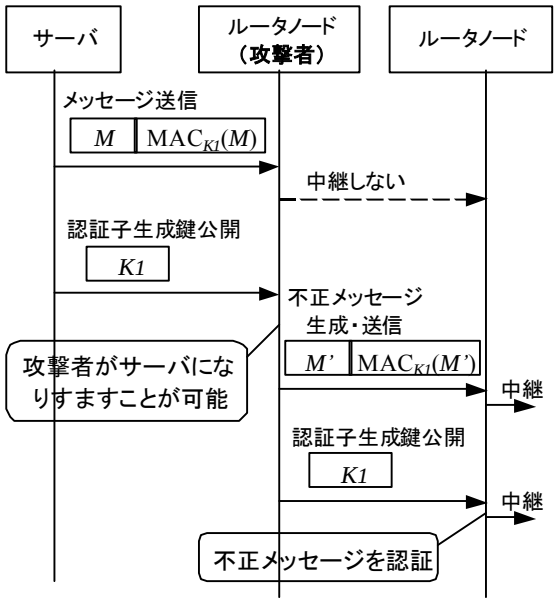


図3：不正なルータノードによるサーバへのなりすまし

サーバが発信したブロードキャストメッセージに対する受信確認を，効率良くかつセキュアに収集する方式について紹介する．

4．2．1 受信確認を得ることの問題点

マルチホップ通信環境において，サーバがブロードキャストメッセージの受信確認を行うには，次のような問題点がある．

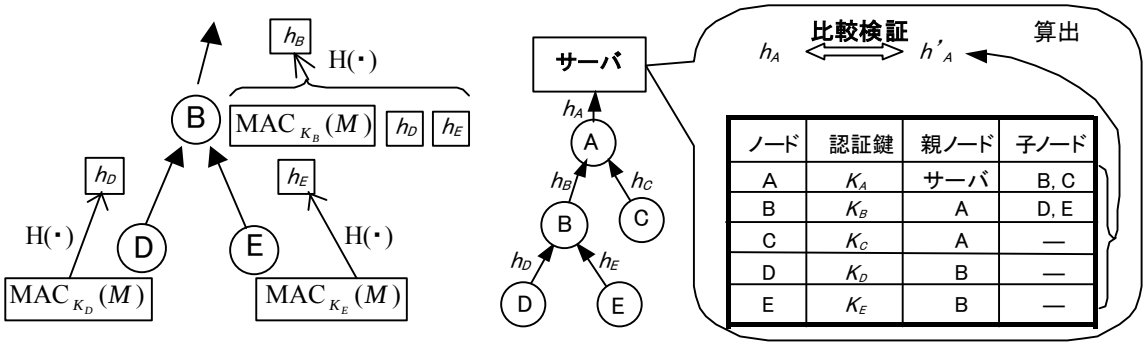
- 膨大な数のノードが存在するセンサネットワークシステムにおいて，受信確認の返信は，ネットワークの通信オーバヘッドが大きい．
- 受信確認メッセージに信憑性がない．（例えば，不正なルータノードが受信確認を偽造している可能性がある．）

4．2．2 Per-Hop Hashing の概念を応用した受信確認方式

Ariadne [1]は，A.Perrig らにより提案されたセキュアルーティング方式である．この論文で紹介されている Per-Hop Hashing の概念を，マルチホップ環境における受信確認情報の生成に応用した[2]．この方式では，サーバと全ノードが，認証鍵（各ノードがサーバと１対１で共有する鍵）とルート情報を共有することを前提とする．図４に，Per-Hop Hashing の概念をマルチホップツリー構造に応用した受信確認方式の概念図を示す．図４において，M はサーバが発信したブロードキャストメッセージを示し，K_A, K_B, K_C, K_D, K_E と，h_A, h_B, h_C, h_D, h_E はそれぞれ，ノード A, B, C, D, E の認証鍵と，各ノードが生成する受信確認を示す．

4．2．2．1 ノードによる受信確認の生成

図４(a)にノードによる受信確認の生成例を示す．各ノードは，自身の親ノードと子ノードを把握している．各ノードは，メッセージの受信をサーバに証



(a) ノードによる受信確認の生成例　　(b) サーバによる受信確認の検証例

図4: Per-Hop Hashingの概念をマルチホップツリー構造に応用した受信確認方式

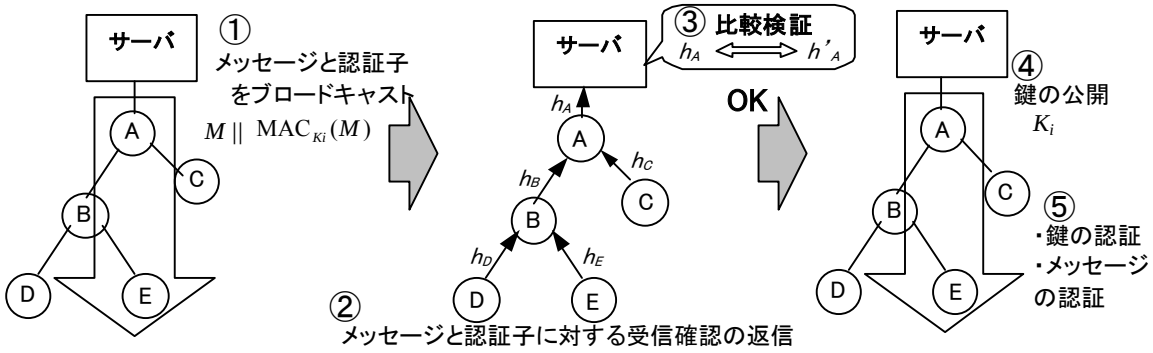


図5: 提案方式の動作概要図

明するために，受信したメッセージに対する認証子を，自身の認証鍵を用いて生成し，それをメッセージに対する受信確認情報とする．各ルータノードでは，自身が生成した認証子と子ノードの受信確認とを重畳したものを自身の受信確認として，親ノードに返信する．ノードXの生成する受信確認 h_X を式(1)に示す．

$$h_X = \mathrm{H}(\mathrm{MAC}_{K_X}(M) \{ \| \text{[子ノードの受信確認]} \| \cdots \}) \quad (1)$$

ここで，$\mathrm{MAC}_{K_X}(\cdot)$ はノードXの認証鍵 K_X を用いた認証子生成アルゴリズム，H(・)はハッシュ関数，‖はビット列の連結，”{‖[子ノードの受信確認]‖…}” はノードXがルータノードである場合にノードXの子ノードが生成する受信確認を示す．

4．2．2．2 サーバによる受信確認の検証

図4(b)にサーバによる受信確認の検証例を示す．サーバは，図4(b)に示す表のように，管理下の全ノードの認証鍵とルート情報を把握するためのテーブルを持つ．サーバは，自身が発信したブロードキャストメッセージ M と，管理テーブルより，ノードが生成するのと同じ手順で受信確認を算出できる．サーバはノードから返信された受信確認 h_A と，算出した受信確認 h'_A が一致するかどうかを検証することで，ブロードキャストメッセージ M が全ノードに届いたか否かを判断する．

4．2．3 方式の特長

本方式は，メッセージの受信確認と共に，サーバが把握するネットワーク構造に変化がないことを確かめることができる．

メッセージの受信確認は，各ルータノードで全子ノードの受信確認を重畳しながら返信するため，各ルータノードにおける受信確認の中継送信回数は 1 回のみである．また，ノード毎にハッシュ（データ圧縮）するので，そのデータサイズは受信を証明するノード数に依存しない．よって，個々のノードがそれぞれ受信確認を送信する場合に比べて，通信のオーバヘッドが抑えられる．

また，受信確認の正当性は，サーバと各ノードが１対１で共有する認証鍵で保証する．よって，任意のノードが出力する受信確認情報を偽造するには，その受信確認を重畳している全ノードの認証鍵を入手しないと困難である．

この方式は，受信確認を重畳するノード数が多いほど受信確認返信のオーバヘッド抑制効果が大きく，攻撃者が受信確認を偽造するのに必要な認証鍵の数も多くなる．よって，センサネットワークのように膨大な数のノードが存在する環境を活かした方式である．

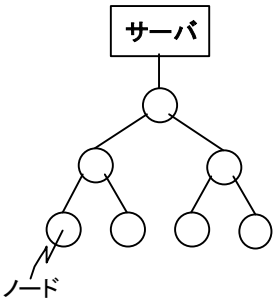
4．3 提案方式の動作とセキュリティ考察

図５は，従来方式である One-way key chain を用いたメッセージ認証と，４．２節で説明した受信確認方式を組み合わせたメッセージ認証方式の動作概要図である．

表1：各種ブロードキャストメッセージ認証方式におけるサーバへのなりすまし攻撃に対する耐性

（※ タイミングにより不正可能）

	共通鍵方式	One-way key chain方式	μTESLA（時刻同期が必要）	提案方式（受信確認が必要）
メッセージ認証鍵の公開（漏洩）	×	△※	○	○
不正なルータノードの存在	×	×	○	○



通信方式 – ZigBee(IEEE802.15.4)規格, 最大ビットレート: 250 [kbps]

ブロードキャスト	ランダム時間(0～64 [ms])後に Unslotted CSMA-CA
受信確認の返信	Unslotted CSMA-CA + ACK

図6：提案方式の処理時間の考察に用いたネットワークモデルと通信方式

提案方式では，３．１節の図２③で示した鍵の公開を，サーバが受信確認を得ることで行うことを特徴とする．

One-way key chain の各鍵で複数のメッセージを認証するように既定する場合は，それら全てのメッセージの受信確認を得た後で，認証子生成鍵を公開する．サーバが鍵を公開した時には，正当なメッセージは既にノードに受信済みである．ノードは公開された鍵を用いて既定数のメッセージのみを認証する．もし，攻撃者が，公開された鍵情報をノードより先に知り，不正データをネットワークに投入したとしても，ノードは，受信が後であった不正データを，既定数より多いデータとして排除できる．

共通鍵暗号系で実現する各種ブロードキャストメッセージ認証方式（従来の共通鍵方式[サーバと全ノードが予め共通の鍵を持つ方式]，One-way key chain を用いた方式，μTESLA[3]，提案方式）について，サーバへのなりすまし攻撃に対する耐性を比較した結果を表１に示す．提案方式は受信確認の偽造が困難という前提で，マルチホップ環境においても攻撃者によるサーバへのなりすましが困難なメッセージ認証方式である．

5 提案方式の処理時間についての考察

本章では，提案方式の処理時間について考察する．サーバがブロードキャストする更新データのサイズを 10 [KByte]，認証子と受信確認情報を全て 8 [Byte]とした．

まず，各データの伝送時間について，机上計算で見積もりを立てる．本考察で想定するネットワークモデルと通信方式を図６に示す．ネットワークモデルには，子ノードの数が２，深さ３のマルチホップツリー構造を用いた．通信方式は， ZigBee™*[4] (IEEE802.15.4[5])規格を元に設定した．図６に示す

表2：図6のネットワークモデルにおけるデータ伝送時間の見積もり

	到達時間 [ms]
更新データ(1フルパケットブロードキャスト)	81
更新データ(95パケットブロードキャスト)（サーバの伝送サイクルを 7.0[Hz]と設定）	13455
受信確認(1パケットユニキャスト)（ルータノードが全子ノードから受信確認情報を得るまで）	3.8 ×（子ノード数）

※ ブロードキャストにおけるランダム時間を平均 32 [ms]とする
※ Unslotted CSMA-CAのBack off時間を平均 1.28 [ms]とする
※ 各ノードにおけるパケット処理遅延を0.64 [ms]とする

ネットワークモデルと通信方式を用いてデータの伝送時間を見積もった結果を表２に示す．サーバは 10 [KByte]のデータに 8 [Byte]の認証子を連結したデータを 95 パケットに分割して送信する．サーバの伝送サイクルを 7.0[Hz]と設定し，ブロードキャストにおけるパケットの衝突と隠れ端末問題は回避できるものとした．ただし，ネットワーク外部要因によるパケットロスは想定していない．

次に，実機（図７参照，CPU: ARM-7，クロック数: 16[MHz]）を用いて演算処理時間を計測した．提案方式においてノードが行う演算処理は，データに付加された認証子を検証する処理，受信確認情報として認証子を生成する処理，受信確認情報をハッシュする処理，認証子生成鍵を検証する処理である．これらの処理に費やす時間を計測した結果を表３に示す．ただし，認証子生成アルゴリズムは AES 暗号を用いた CBC-MAC(Cipher Block Chaining-Message Authentication Code)を利用し，ハッシュ関数は AES 暗号を用いた暗号化とビット切り捨てで代用し，一方向性関数は AES 暗号に基づく一方向性関数[7]を用いた．AES 暗号のブロックサイズ，鍵長，One-way key chain の鍵長は全て 16 [Byte]である．

* ZigBeeはKoninklijke Philips Electronics N.V. の登録商標です．

図7：演算処理時間の測定に用いた実機
（CPU: ARM-7, クロック数: 16 MHz）

表3：実機上での演算処理時間測定結果
（データ: 10[KByte], 認証子: 8[Byte], 受信確認情報: 8[Byte]）

	処理時間 [ms]
データの認証子検証処理	617
受信確認（データと認証子の組に対する認証子）生成処理	617
受信確認情報のハッシュ処理	2.6（ルータノード） 1.6（エンドノード）
鍵の検証処理	0.56

表4：提案方式における処理時間の見積もり

処理	処理時間 [ms]
10[KByte]更新データの受信とデータの認証子検証	14072
受信確認の返信	644
認証子生成鍵の受信と検証	73
処理時間合計[ms]	14789

以上，データ伝送時間の見積もり結果と，実機を用いた演算処理時間の計測結果より，提案方式の処理時間を見積もった結果を表４に示す．ただし，サーバによる受信確認情報の算出はノードから受信確認が返信されるまでに実行しているものとし，受信確認情報の検証時間は比較のみのため無視できるとする．表４より，受信確認の返信にかかる時間と，認証子生成鍵の受信・検証にかかる時間の合計は，方式全体の処理時間に対して 5%程度であり，更新データの受信（と認証）にかかる時間が処理時間の大部分を占めていることがわかる．以上より，想定した環境・条件では，更新データの配送信頼性を確保するのにかかる処理時間をどのように抑えるかが，方式全体の処理時間の削減に有効であることがわかる．

7 まとめ

以上，効率良くかつセキュアにメッセージの受信確認を収集する方式を説明し，それを従来方式である One-way key chain を用いたメッセージ認証と組み合わせることで，受信確認を伴った高信頼ブロードキャストメッセージ認証方式を提案した．本方式は，受信確認の偽造が困難という前提の下で，マルチホップ環境においても攻撃者によるサーバへのなりすましに耐性がある．

今後は，実機への実装による評価と，それを反映した改良方式の検討が課題となる．

参考文献

[1] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *MobiCom'02*, Atlanta, Georgia, USA, (2002).

[2] 八百，川本，松村，福永：“センサネットワークのマルチホップツリー構造に適したセキュアな受信確認方式，” 情報処理学会研究報告，2004-MBL-30, pp.69-75(2004).

[3] A. Perrig et al., “SPINS: Security Protocols for Sensor Networks,” *Wireless Networks J.*, vol.8, no.5, pp.521-534, (2002).

[4] ZigBee Alliance, http://www.zigbee.org/

[5] IEEE802.15.4: “Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LRWPANs)”, http://www.ieee802.org/15/pub/TG4.html

[6] A.J. Menezes, P.C.van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Ration: CRC Press, (1997).