Computer Security Symposium 2014
22 - 24 October 2014

センサネットワークにおける署名サイズを抑えた認証付データの放送型通信

坂井 昭仁† 楫 勇一† 伊藤 実†

†奈良先端科学技術大学院大学
630-0192 奈良県生駒市高山町 8916-5
sakai.akihito.rm8,kaji,ito@is.naist.jp

あらまし 多くのセンサネットワークシステムでは，サーバからの放送型通信を有効に活用して各種の機能を実現している．この放送型通信に対して送信者認証機能を付加する事が重要であるが，センサノードは非常に限られた計算資源しか持たないため，電子署名等の汎用技術を利用することは困難である．そこで本研究では，複数のハッシュ連鎖を組み合わせて利用し，放送型通信のデータ認証を安全かつ軽量に実現する．本稿では，著者らが既に提案している方式から，ノードの保持するデータ量を削減する改良方式を検討し，その効果を定量的に評価する．

Data authentication scheme which restrains signature size for broadcast in the sensor networks

Akihito Sakai† Yuichi Kaji† Minoru Ito†

†Graduate school of Information Science, Nara Institute of Science and Technology
8916-5, Takayama, Ikoma, Nara 630-0192, JAPAN
sakai.akihito.rm8,kaji,ito@is.naist.jp

Abstract Data broadcasting is often utilized in a sensor network system, but the authentication of the broadcast data is not a simple issue. The computational resources of sensor nodes are so restricted that common security techniques such as digital signatures may not be available in a sensor network system. Based on the previous work by the authors, this study aims to reduce the size of data that is possessed by nodes, and evaluates its contribution in terms of processing time and energy consumption.

1 はじめに

センサネットワークは，センサノード（ノード）と呼ばれる多数の端末により構成されるネットワークシステムである．とくに，ノード間の通信に無線を利用する無線センサネットワークは，その設置にあたって専用の通信基盤等を構築する必要がないため，気象観測，農業，災害予防，テレメータリング等，従来のネットワークでは対応が困難であった環境での情報収集に威力を発する [4][7]．一般的に，センサノードにおいては省電力化が最重要視されるため，ノードには，非常に限定された機能と資源しか与えられないことも多い．したがって，公開鍵暗号や電子署名に代表されるような，大規模計算が必要となるセキュリティ技術の利用は望ましくないとされている．楕円曲線暗号に代表されるように，計算量の小さな公開鍵暗号等の研究も進め

られているが [5]，それらの成果がセンサノードに対してどのような影響を与えるかは，まだ十分に評価されていない．以上の状況を念頭に，本研究では，サーバと呼ばれる管理者が複数のノードに向けて発信する情報の**データ認証**の問題について議論を行う．センサネットワークの実用的な構成においては，ネットワーク内に特別な端末の存在を仮定し，その端末が，ネットワークの制御や管理を行うと考えるのが自然である．本研究では，そのような端末を**サーバ**と呼ぶことにする．サーバは，ノードが発信する情報の受け手となるだけでなく，必要に応じ，自らノードに対して何らかの情報を発信する．様々なタイプの情報発信が考えられるが，本研究で議論するのは，サーバが複数のノードに対して同一の情報を発信する，いわゆる**放送型通信**の安全性である．放送型通信の中にはグループ鍵の更新，ノードの動作モードの変更のように，ネットワークの動作を大きく左右する重要なものが含まれるケースも多い．もし，サーバになりすました不正者による放送型通信を許してしまうと，ネットワークに致命的な障害が生じる可能性もある．

通常の計算機ネットワークでは，放送型通信のデータ認証は，サーバの**電子署名**を用いて実現することが一般的である．しかし，先に述べたように，電子署名を用いることはセンサネットワークにおいて好ましい選択肢ではない．一対一の通信であれば，電子署名の代替として**データ認証子** (message authentication code, MAC) を用いることも考えられるが，三者以上が関与する通信では，MAC 鍵を持つ受領者（たとえば，攻撃者に乗っ取られたノード）が不正を働く可能性があるため，データ認証子は機能しない．

本研究では，２本のハッシュ連鎖を対向させて利用することで，安全かつ軽量に，放送型通信におけるデータ認証を実現する手段について考える．著者らが以前提案した方式から，ノードの保持するデータサイズを削減する方式を検討し，その効果を評価する．

2　関連研究

Perrig らは SPINS と呼ばれる枠組みの中で，**ハッシュ連鎖**を用いた放送型データ認証方式を提案している [1]．Perrig らの方式では，ハッシュ連鎖の終端の値が事前に公開されており，ハッシュ連鎖の途中の値が，ある一定期間の MAC 鍵の役割を果たす．規定の期間が過ぎると，それまで使われていた MAC 鍵は公開され，ハッシュ連鎖を一段遡ったところにあるハッシュ値が，次の期間の MAC 鍵として使われることになる．各ノードは，MAC 鍵が公開されるまで MAC 付きデータを保管しておき，公開された MAC 鍵を使って，MAC の整合性を確認することになる．このように，ハッシュ連鎖の値を時間差で公開していくことで，「MAC の検証はできるが生成はできない」仕組みを構成している．ただし，この方式では，サーバが MAC 鍵を公開するまでデータ認証を完了できないので，ノードに著しい負担を強いることになる．

八百らは，MAC の検証に必要な情報を事前にノードに送付し，その後に，保護したいデータを送信する 2 段階のデータ認証方式を提案している [8]．この方式では，最初に鍵情報を送付するためのユニキャスト的な通信が必要となるが，鍵情報のサイズはデータに比べて非常に小さいため，単純なユニキャスト方式と比べた場合，全体の通信量を削減することができる．また，データ部分の流通に関して，センサネットワークの運用に則した「データ再送」が可能となっている等，センサネットワークでの運用を十分に意識した方式であると言える．

著者らは，２本のハッシュ連鎖を対向させてデータを保護する仕組みを提案している [6]．この方式では，攻撃者がサーバから受信したデータを用いて改ざんを試みても，どちらか片方のハッシュ連鎖を逆にたどる計算が必要となり，データの改ざんが困難となっている．一方で，ノードには少なくない回数のハッシュ計算を課している点や，改ざん許容確率を小さくするほど，ノードが保持するデータ量が増大してしまう問題点が存在している．

3　提案方式

本節では，最初に 1 組のハッシュ連鎖組を利用する基本方式を示し，提案する仕組みが安全性を保証する原理について説明を行う．基本方式には，不正者によるデータの偽造や改ざんを防ぐ効果があるが，基本方式を単体で用いたのでは，安全性と計算量とを両立することが困難である．そこで，本節後半では，基本方式を複数組み合わせ，かつ，ノードが保持するデータ量を削減する応用方式を考え，検討を行う．

3.1　基本方式

提案する認証方法の特徴は 2 つの一方向ハッシュ連鎖を用いることである．なお，以降では n をハッシュ連鎖の長さ，h を値域が $\{0, 1, \ldots, n-1\}$ である一方向ハッシュ関数，f を任意の一方向ハッシュ関数とする．一方向ハッシュ関数 f は，ハッシュ連鎖の構成に用いられる．以下では，$f^0(x) = x$, $f^{n+1} = f(f^n(x))$ と表記する．

提案する基本方式は,「初期情報の配布」,「認証付データの放送型通信」,「ノードによる検証処理」の 3 つの構成要素からなる．各構成要素における計算や操作について，順を追って説明する．

初期情報の配布　サーバは，シードと呼ばれる二つの乱数値 s_L, s_R を選択し，これらのシードを始点として長さ n のハッシュ連鎖 $t_L = f^n(s_L), t_R = f^n(s_R)$ を生成する．これらのハッシュ連鎖の終端 t_L, t_R は，安全な方法で各ノードに配布されるものとする．

認証付データの放送型通信　サーバは新たなシード $s_L^{'}$, $s_R^{'}$ を選び，初期情報の配布の際と同様にしてハッシュ連鎖を構成し，$t_L^{'} = f^n(s_L^{'})$, $t_R^{'} = f^n(s_R^{'})$ を生成する．次に m と $t_L^{'}, t_R^{'}$ を用い $i = h(m, t_L^{'}, t_R^{'})$ を計算する．この i の値と，これまで使われていたシード s_L, s_R を用いてハッシュ連鎖の計算を行い，$\langle m, t_L^{'}, t_R^{'}, f^i(s_L), f^{n-i}(s_R)\rangle$ を各ノードに対して放送する．さらに，現在保管しているシード s_L, s_R を，いま新たに選んだ $s_L^{'}, s_R^{'}$ に置き換える．

ノードによる検証処理　各ノードは，サーバから送られてきたデータ $\langle a, b_L, b_R, c_L, c_R\rangle$ に対し，各要素の整合性が取れているかどうかを検証する．具体的には，はじめに $i = h(a, b_L, b_R)$ を計算し，t_L と $f^{n-i}(c_L)$, t_R と $f^i(c_R)$ が一致するか確認する．一致すればデータを受理し、ノードが保持している情報 t_L, t_R を b_L, b_R に置換する．一致しなければデータを破棄する．

基本方式の最大の特徴は，2 本のハッシュ連鎖を相補的に用いている点である．攻撃者が認証付放送データを盗聴し，悪意を持って改変しようとしても，どちらか片方のハッシュ連鎖を逆にたどるような計算が必要となる．ハッシュ連鎖を逆にたどることは難しいため,（一定の確率で）データの偽造や改変を防止することができる．このことについて，もう少し具体的に議論するため，$\langle a, b_L, b_R, c_L, c_R\rangle$ を入手した攻撃者が，攻撃者は a, b_L, b_R の 3 要素を $a^{'}, b_L^{'}, b_R^{'}$ にデータを改ざんしようとする場合，改ざんが成功する条件は $j = h(a', b'_L, b'_R)$ に対し，攻撃者が $f^j(s_L)$, $f^{n-j}(s_R)$ の両方を計算できるときのみである．これらの値を計算するために，攻撃者は，盗聴したデータに含まれていたハッシュ値 $f^i(s_L)$, $f^{n-i}(s_R)$ を利用する可能性があるが，2 つのハッシュ値を正しく計算できるのは $j = i$ のとき，かつ，そのときのみであり，その確率は $1/n$ である（厳密には，攻撃者が無作為に作成した値が正しいハッシュ値と偶然一致する確率についても考慮する必要があるが，その確率は $1/n$ に比べて微小であるため，無視しても良い）．n を大きな値にすれば，改ざん成功確率を小さくすることができるが，長いハッシュ連鎖を取り扱う必要が生じるため，サーバおよびノードの計算量が増大してしまう．

3.2　応用方式

基本方式の安全性と効率のトレードオフ点を改善するため，ハッシュ連鎖の組を m 組用意し，その m 組を組み合わせて利用することを考える．ノードにおいては，m 組の連鎖すべてについて整合性が確認できた場合のみデータを

受理する．この場合，サーバおよびノードにおけるハッシュ計算の回数は m に比例して大きくなるが，改ざん成功確率は m に対して指数的に小さくなることが期待できる．一般には，ハッシュ連鎖組の長さを同一に設定する必要はなく，逆に，ハッシュ連鎖組を戦略的に定めることにより，安全性と効率の関係を制御することができる．ここでは，ハッシュ連鎖組を複数用いる方式を，単に応用方式と呼ぶことにする．応用方式では，使用するハッシュ連鎖組の個数 m，$k(1 \leq k \leq m)$ 組目のハッシュ連鎖組の長さ n_k，m 個の一方向ハッシュ関数 $h_1, h_2, \ldots, h_m$(ただし，h_k の値域は $\{0, 1, \ldots, n_k - 1\}$)，任意の一方向ハッシュ関数 f と事前にパラメータを準備しておく必要がある．

初期情報の配布においては，サーバは，m 組のシード $s_{L,k}, s_{R,k}(1 \leq k \leq m)$ を準備し，各連鎖の終端の値 $t_{L,k}, t_{R,k}$ をノードに配布しておく．ただし，$t_{L,k} = f^{n_k}(s_{L,k})$，$t_{R,k} = f^{n_k}(s_{R,k})$ である．認証付データの送信においても，m 組のシード $s'_{L,k}, s'_{R,k}$ を準備し，それぞれに対応する $t'_{L,k}, t'_{R,k}$ を計算する．さらに，各 $1 \leq k \leq m$ に対して $i_k = h_k(m, t'_{L,k}, t'_{R,k})$ を計算し，

$$\begin{aligned}\langle m, t'_{L,1}, t'_{R,1}, ..., t'_{L,m}, t'_{R,m},\\ f^{i_1}(s_{L,1}), f^{n_1-i_1}(s_{R,1}), \ldots,\\ f^{i_m}(s_{L,m}), f^{n_m-i_m}(s_{R,m}))\rangle\end{aligned}$$

を放送する．ノードによる検証では，m 組のハッシュ連鎖組のすべてについて，値の整合性が取れているかどうかを確認する．一つでも整合性の取れないハッシュ連鎖組がある場合は，その時点で受信データを破棄してよいため，すべてのハッシュ連鎖組をたどる必要はない．

3.3 ノードの保持データ量削減法

ここで，ノードが保持するデータ量について考える．あるハッシュ連鎖組において，ノードが受信データを検証するためには，サーバ側で作成するハッシュ連鎖の終端の 2 つの値 t_L, t_R を保持しておかなければならない．ここで，t_L, t_R を個別に保持するのではなく，排他的論理和をとることで 2 つのハッシュ値を 1 つにまとめ，

$$t_{LR} = t_L \oplus t_R$$

と定義される 1 個の値 t_{LR} をノードに保持させることを考える．3.1 節におけるノードによる検証処理では，受信データ $\langle a, b_L, b_R, c_L, c_R\rangle$ から計算されたハッシュ値 $f^{n-i}(c_L), f^i(c_R)$ に対して，ノードが保持しているハッシュ値 t_L, t_R と比較を行い，$t_L = f^{n-i}(c_L)$ と $t_R = f^i(c_R)$ をそれぞれ比較してデータ認証を行っていたが，この変更に伴って，ノードによる検証処理では，

$$t_{LR} = f^{n-i}(c_L) \oplus f^i(c_R)$$

のとき，かつそのときのみ，受信データを受理する．このようにハッシュ値の取り扱い方法を変更することで，ノードが保持するメモリ量を 1/2 に削減することができる．

上記では，1 組のハッシュ連鎖の終端の値 2 つを 1 つにまとめることを考えたが，一般には，任意の正整数 z に対し，z 組のハッシュ連鎖の終端値 $2z$ 個を 1 つにまとめることができる．以下では，ハッシュ連鎖の終端値が 1 個にまとめられた $2z$ 個のハッシュ連鎖の集合をハッシュ連鎖グループ，または単にグループと呼ぶことにする．グループごとにハッシュ値をまとめることで，ノードが保持するデータ量は，前節で述べた方式に比べ $1/2z$ の量となる．その一方，ノードにおける検証処理では，同一グループに属するハッシュ連鎖のすべてに対し，受信データから計算される連鎖の終端値を求める必要があるため，ノードにおける計算量が増加する可能性がある．

3.4 応用方式における計算量の制御

ここでは，応用方式を利用する際の計算量について検討を行う．ただし，ここでは議論を簡単にするため，ノードが受信データを検証するために必要なハッシュ計算の回数を考え，さらに，ハッシュ連鎖の総組数は，1 つのハッシュ連鎖グループの組数の倍数であるとする，ノードが受信データを検証する際には，k 番目のハッシュ連鎖組に対し，$(n_k - i_k) + i_k = n_k$ 回のハッ

シュ連鎖計算が必要となる．もし受信データが正しいものである場合，m 組のハッシュ連鎖組のすべてに対して検証操作を行うことになるため，ノードにおけるハッシュ計算の回数は

$$\theta_{acc} = n_1 + \cdots + n_m$$

となる．前節で述べたとおり，ノードにおける検証処理では，1 つのグループに属するすべてのハッシュ連鎖に対し，その終端値を計算する必要がある．仮に，グループ内に z 組のハッシュ連鎖組が存在し，それぞれの長さが $n_1, \ldots, n_z$ で与えられるとすると，このグループに関する整合性検査には $n_1 + \cdots + n_z$ 回のハッシュ計算が必要となる．攻撃者の偽造データが検出される確率は $1 - 1/(n_1 \cdots n_z)$ であり，この場合はデータを破棄して検証操作を終えることができるが，その一方で，$1/(n_1 \cdots n_z)$ の確率で不正を見逃す可能性がある．この場合は，次の z 組分のハッシュ連鎖を一斉に整合性の検査を行う必要があり，$n_{z+1} + \cdots n_{2z}$ 回のハッシュ計算が必要となる．以下同様にして議論を行うと，受信データが不正なものであった場合，ノードにおいて必要となるハッシュ計算の回数の期待値は

$$\begin{aligned}\theta_{rej} &= (n_1 + \cdots + n_z) + \frac{n_{z+1} + \cdots + n_{2z}}{n_1 \cdots n_z} \\ &\quad + \cdots + \frac{n_{m-z+1} + \cdots + n_m}{n_1 \cdots n_{m-z}}\end{aligned}$$

により与えらえる．不正データが m 組のハッシュ連鎖組の整合性検査をすり抜けた場合にのみデータの改ざんに成功するが，その確率は，

$$p = \frac{1}{n_1}\frac{1}{n_2}\cdots\frac{1}{n_m}$$

によって与えられる．θ_{rej} を最小化するためのグループ内の連鎖組の長さについて，以下の定理を示すことができる．

定理 1. 与えられた改ざん確率に対し，$\theta_{acc}, \theta_{rej}$ が最小となるのは，グループ内の z 組のハッシュ連鎖の長さが全て等しいときである．

証明．m 組のハッシュ連鎖組を z 組ずつにグループ分けし，各グループを $G_1, \ldots, G_{m/z}$ と書く．グループ G_i には $iz-z+1, \ldots, iz-z+2, iz-z+z$ 組目のハッシュ連鎖組が属していることになる．ここで，θ_{rej} が最小となるよう各グループに属するハッシュ連鎖組の長さを適当に定めたとする．グループ G_i における検証に必要となるハッシュ計算の回数を γ_i とし，グループ G_i における検証で不正を見逃してしまう確率を π_i と書くと，θ_{acc} は，

$$\theta_{acc} = \gamma_1 + \gamma_2 + \cdots + \gamma_{\frac{m}{z}}$$

であり，θ_{rej} は，

$$\begin{aligned}\theta_{rej} &= \gamma_1 + \frac{\gamma_2}{\pi_1} \\ &\quad + \cdots + \frac{\gamma_{\frac{m}{z}}}{\pi_1\pi_2\cdots\pi_{\frac{m}{z}-1}}\end{aligned}$$

となる．ここで，あるグループ G_k に属するハッシュ連鎖組の長さが同一でないと仮定する．このときのグループ G_k の改ざん確率，ハッシュ計算回数 γ_k, π_k は，

$$\begin{aligned}\gamma_k &= n_{kz-k+1} + n_{kz-k+2} + \cdots + n_{kz} \\ \pi_k &= \frac{1}{n_{kz-k+1}}\frac{1}{n_{kz-k+2}}\cdots\frac{1}{n_{kz}}\end{aligned}$$

となる．ここで，π_k の値を変えずに G_k に属するハッシュ連鎖組の長さを同一にした場合のハッシュ計算回数を $\gamma_k^{'}$ とすると，

$$\begin{aligned}\gamma_k &= n_{kz-k+1} + \cdots + n_{kz} \\ &= z\frac{n_{kz-k+1} + \cdots + n_{kz}}{z} \\ &\geq z\left(n_{kz-k+1}\cdots n_{kz}\right)^{\frac{1}{z}} \\ &= z\left(\frac{1}{\pi_k}\right)^{\frac{1}{z}} \\ &= z(n_{kz-k+1}^{'}\cdots n_{kz}^{'})^{1/z} \\ &= z\frac{n_{kz-k+1}^{'} + \cdots + n_{kz}^{'}}{z} = \gamma_k^{'}\end{aligned}$$

が成り立つ．ここで不等号は，相加･相乗平均の性質より導かれる．ここで，仮定より，$n_{kz-k+1} + \cdots + n_{kz}$ の値は全てが同一ではなく，したがって γ_k は $\gamma_k^{'}$ より真に大きい．これは $n_{kz-k+1} + \cdots + n_{kz}$ が θ_{rej} を最小とするという仮定と矛盾する．よってグループ内のハッシュ連鎖長は同一でなければならず本定理が成立する． □

定理 1 より，グループ内のハッシュ連鎖組を等長にすると $\theta_{acc}, \theta_{rej}$ および p は

$$\begin{aligned}\theta_{acc} &= zn_z + zn_{2z} + \cdots + zn_m \\ \theta_{rej} &= zn_z + \frac{zn_{2z}}{n_z^z} \\ &\quad + \cdots + \frac{zn_m}{(n_z n_{2z} \cdots n_{m-z})^z} \quad (1) \\ p &= \frac{1}{n_z^z}\frac{1}{n_{2z}^z}\cdots\frac{1}{n_m^z} \quad (2)\end{aligned}$$

と書くことができる．以上を踏まえて，θ_{rej} を最小化するとき，以下の定理を示すことができる．

定理 2. m, p, z および $g(= m/z)$ が与えられたとき，θ_{rej} の最小値は

$$\begin{aligned}&\min(\theta_{rej}) = \sigma\left(g, \frac{1}{p}, m, z\right) \\ &= \frac{(z+1)^g - 1}{(z+1)^{g-1}} \\ &\cdots \left((z+1)^{\frac{(z+1)^g - gz - 1}{z}} \frac{1}{p}\right)^{\frac{1}{(z+1)^{g-1}}}\end{aligned}$$

として与えられる．

証明. 以下では表記を簡単にするために $q = 1/p$ と置く．したがって，式 (2) は

$$q = n_z^z n_{2z}^z \cdots n_m^z$$

と書くことができる．また，θ_{rej} の最小値を導出するにあたり，$\sigma(g, q, m, z)$ を

$$\min_{n_z^z \cdots n_m^z = q} \left(zn_z + \cdots + \frac{zn_m}{(n_z n_{2z} \cdots n_{m-z})^z}\right)$$

と定義する．これは，m 組のハッシュ連鎖組を使い，改ざん許容確率を $1/q$ とする場合のハッシュ計算の回数の最小値 (式 (1) の最小値) であり，$\min(\theta_{rej}) = \sigma(g, q, m, z)$ として与えられる．詳細は省略するが，比較的小さな m の値について $\sigma(g, q, m, z)$ を求め，一般化すると，

$$\begin{aligned}&\sigma(g, q, m, z) \\ &= \frac{(z+1)^g - 1}{(z+1)^{g-1}} \\ &\cdots \left((z+1)^{\frac{(z+1)^g - gz - 1}{z}} q\right)^{\frac{1}{(z+1)^{g-1}}} \quad (3)\end{aligned}$$

となることが予測される．この予測が正しいことを数学的帰納法を用いて証明する．

$(i) g = 2$ のときは，$q = n_z^z n_m^z$ であり，したがって式 (1) は

$$\theta_{rej} = zn_z + \frac{q^{\frac{1}{z}}}{n_z^{z+1}} \quad (4)$$

と書くことができる．最小値を求めるため，式 (4) を n_z で微分して 0 と置くと

$$n_z = ((z+1)q)^{\frac{1}{z^2+2z}}$$

が得られ，これから n_m も定まり．この n_z, n_m の値が 式 (1) を最小化するため，

$$\sigma(2, q, m, z) = \frac{z^2 + 2z}{z+1} ((z+1)q)^{\frac{1}{z^2+2z}}$$

となる．

$(ii) g = \alpha$ のとき $\sigma(\alpha, q, m, z)$ が

$$\frac{(z+1)^\alpha - 1}{(z+1)^{\alpha-1}} \left((z+1)^{\frac{(z+1)^\alpha - \alpha z - 1}{z}} q\right)^{\frac{1}{(z+1)^\alpha - 1}}$$

が成立すると仮定し，$m/z = \alpha + 1$ のとき，$\sigma(\alpha+1, q, m, z)$ が

$$\begin{aligned}&\frac{(z+1)^{\alpha+1} - 1}{(z+1)^\alpha} \\ &\cdots \left((z+1)^{\frac{(z+1)^{\alpha+1} - (\alpha+1)z - 1}{z}} q\right)^{\frac{1}{(z+1)^{\alpha+1} - 1}} \quad (5)\end{aligned}$$

となることを示せばよい．$m/z = \alpha + 1$ のときは，$q = n_z^z n_{2z}^z \cdots n_{\alpha+1}^z$ であり，θ_{rej} は

$$\theta_{rej} = zn_z + \frac{zn_{2z}}{n_z^z} + \cdots + \frac{zn_{(\alpha+1)}}{n_z^z n_{2z}^z \cdots n_\alpha^z}$$

である．ここで，$n_{2z}, \cdots, n_{\alpha+1}$ の選択は，$\frac{q}{n_z^z} = n_{2z}^z n_{3z}^z \cdots n_{\alpha+1}^z$ の条件の下で

$$\left(n_{2z} + \frac{1}{n_{2z}^z}\left(\cdots \frac{1}{n_{\alpha-1}^z}\left(zn_\alpha + \frac{zn_{\alpha+1}}{n_\alpha^z}\right)\right)\right)$$

を最小化するよう成されなければならない．したがって，θ_{rej} の最小値は

$$\begin{aligned}&zn_z + \frac{1}{n_z^z}\sigma\left(\alpha, \frac{q}{n_z^z}\right) \\ &= zn_z + ((z+1)^\alpha - 1) \\ &\cdots (z+1)^{\frac{(z+1)^\alpha (1 - \alpha z + z) - 1 - z}{z(z+1)^\alpha - z}} q^{\frac{1}{(z+1)^\alpha - 1}} n_z^{\frac{-z(z+1)^\alpha}{(z+1)^\alpha - 1}} \quad (6)\end{aligned}$$

の最小値として与えられる．式 (6) を n_z で微分して 0 と置くと，

$$n_z = \left((z+1)^{\frac{(z+1)^{\alpha+1}-(\alpha+1)z-1}{z}} q\right)^{\frac{1}{(z+1)^{\alpha+1}-1}} \quad (7)$$

が得られる. この値を式 (6) に代入すると，

$$\begin{aligned}&\sigma(\alpha+1, q, m, z)\\ &= \frac{(z+1)^{\alpha+1}-1}{(z+1)^{\alpha}}\\ &\cdots \left((z+1)^{\frac{(z+1)^{\alpha+1}-(\alpha+1)z-1}{z}} q\right)^{\frac{1}{(z+1)^{\alpha+1}-1}}\end{aligned}$$

となり，式 (5) と一致した．以上より，

$$\begin{aligned}&\sigma(g, q, m, z)\\ &= \frac{(z+1)^{g}-1}{(z+1)^{g-1}}\\ &\cdots \left((z+1)^{\frac{(z+1)^{g}-gz-1}{z}} q\right)^{\frac{1}{(z+1)^{g}-1}}\end{aligned}$$

であり，

$$\begin{aligned}&\min(\theta_{rej}) = \sigma\left(g, \frac{1}{p}, m, z\right)\\ &= \frac{(z+1)^{g}-1}{(z+1)^{g-1}}\\ &\cdots \left((z+1)^{\frac{(z+1)^{g}-gz-1}{z}} \frac{1}{p}\right)^{\frac{1}{(z+1)^{g}-1}} \quad (8)\end{aligned}$$

であることが証明された． □

定理 2 の証明の過程より，θ_{rej} を最小化するためには，最初に $n_1, \ldots, n_z$ の値を式 (7) にしたがって定め，残ったハッシュ連鎖の長さを順々に定めていけばよいことがわかる．ここで，式 (7) の右辺を取り出し，

$$\begin{aligned}&\rho(g, q, m, z) \quad (9)\\ &= \left((z+1)^{\frac{(z+1)^{g}-gz-1}{z}} q\right)^{\frac{1}{(z+1)^{g}-1}} \quad (10)\end{aligned}$$

と書くことにすると，以下の系が得られる．

系 1. ハッシュ連鎖組の個数が m，改ざん確率が $1/q$，および z 組ずつハッシュ連鎖組の整合性検査を行うとき，θ_{rej} を最小化する $n_1, \ldots, n_m$ の値は

$$\begin{aligned}&n_{jz-z+1}, \ldots, n_{jz-z+z}\\ &= \rho\left(g-j+1, q\prod_{l=1}^{j-1}\frac{1}{n_{lz}^{z}}, m-jz+z, z\right)\\ &n_{n-z+1}, \ldots, n_m = \left(\frac{q}{n_z^z n_{2z}^z \cdots n_{m-z}^z}\right)^{\frac{1}{z}}\end{aligned}$$

として与えられる．

証明. 定理 2 の証明と式 (10) の定義より明らか． □

4 性能評価

前節では，ノードが保持するハッシュ値をまとめることによって，署名サイズを抑え，θ_{acc}, θ_{rej} を最小化する手法について議論した．本節では，グループのサイズが θ_{acc},θ_{rej} にどのような影響を与えるか評価する．さらに，提案手法と一般的に用いられているデジタル署名を消費電力，処理速度の観点から比較を行う．

4.1 数値評価

3.3 節で述べたとおり，z 組のハッシュ連鎖組で 1 個のグループを構成すると，ノードが保持するデータ量が $1/2z$ となる．逆に，ノードのデータ量を一定にすると，従来の $2z$ 倍の組数のハッシュ連鎖組が使用でき，安全性と効率のトレードオフ点を改善することができる．ここでは，ノードのデータ量は同一のままグループサイズを変化させ，θ_{acc},θ_{rej} の値を比較する．比較を行う条件として，ハッシュ連鎖の総組数を $m = 32$，改ざん許容確率を $p = 2^{-128}$，グループサイズを $z = 1, 2$ として与える．すると，θ_{acc},θ_{rej} は表 1 のようになる．

まとめるハッシュ値の数を増加させると，θ_{acc} が大幅に減少することがわかる．一方で，θ_{rej} はわずかに増加している．これは，一度に検査しなければならないハッシュ連鎖組の数が増加するためである．

表 1: ハッシュ計算回数

z	m	θ_{acc}	θ_{rej}
なし	32	3768631876229	4.500
1	64	297477	4.004
2	128	256	5.333

表 2: 検証 1 回あたりの消費電力，処理速度

	消費電力	処理速度
提案手法	2.417mJ	27,853cycle
1024bit-RSA	15.970mJ	130,000cycle

4.2 デジタル署名との比較

一般的な計算機ネットワークでは，放送型通信の認証方式としてデジタル署名が一般的であると考えられる．この節ではデジタル署名の 1 つである 1024bit-RSA 署名と提案手法を対象に，ノードによる検証 1 回あたりにかかる消費電力，処理速度の観点から比較を行う．提案手法で用いられている一方向ハッシュ関数 f に関しては，MD5 を使用する．また，1024bit-RSA 署名と MD5 の消費電力，処理速度に関しては既存研究である [2][3] から算出する．提案手法における一方向ハッシュ関数 f の検証 1 回あたりのハッシュ計算の回数は正当な受信データの認証にかかる $\theta_{acc} = 256$ を用いる．提案手法と 1024bit-RSA 署名の消費電力，処理速度は表 2 のようになる．提案手法の方が消費電力，処理速度共に優れており，消費電力では約 85 %削減することができ，処理速度は約 79 %高速にすることができる．

5 まとめ

本論文では，センサネットワークにおける署名サイズを抑えた認証付データの放送型通信の方式を提案した．提案した方式では，ノードが保持する検証用のデータ，すなわちハッシュ連鎖組の終端のハッシュ値をまとめることによって署名サイズの削減を実現している．これにより，署名サイズを任意に定めると，著者らが提案した既存方式 [6] と比べ，より多くのハッシュ連鎖組を用いることができ，ハッシュ計算の回数を削減することができる．一方で，今回提案した方式では，まとめるハッシュ値の数を一定にしている．今後はまとめるハッシュ値の数を柔軟に定めることによって，性能を最適化する方法を検討する．

参考文献

[1] A.Perring, R.Szewczyk, V.Wen, D.Culler, J.D.Tygar., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks Journal., vol.8, no.5, pp.521-534, 2002.

[2] Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html

[3] N.R.Potlapally, S.Ravi, A.Raghunathan, N.K.Jha, Analyzing the Energy Consumption of Security Protocols, Proc. of the 2003 Intl. Symp. on Low Power Electrinics and Design, Seoul, Korea, pp.30-35, 2003.

[4] J.Yick, B.Mukherjee, D.Ghosal., “Wireless Sensor Network Survey,” Computer Networks: The Intl. J. of Computer and Telecommunications Networking, vol.52, no.12, pp.2292-2330, 2008.

[5] 岡本龍明，内山成憲，“公開鍵暗号の最近の話：楕円曲線暗号の安全性について”，情報処理学会学会誌，vol.39，no.12，pp.1252-1257，1998.

[6] 坂井昭仁，楫勇一，伊藤実，“センサネットワークにおける放送型通信に適したデータ認証方式”，情報セキュリティ研究会，A-3，2014.

[7] 阪田史郎，ユビキタス技術センサネットワーク，オーム社，2006.

[8] 八百健嗣，中嶋純，福井潔，“低リソースセンサノード向け代理配信可能データ認証手法の評価”，2014 年暗号と情報セキュリティシンポジウム，1D1-1，2014.