マルチキャストソフトウエア更新情報の中継器による代理配信を可能とする無線マルチホップシステム用データ認証技術

八百　健嗣　　中嶋　純
福井　潔

920MHz帯無線マルチホップネットワークは、近年期待されるM2M（Machine-to-Machine）システムの末端に位置付けられるネットワークであり、家庭やオフィスにおけるエネルギーマネージメント、構造物のヘルスモニタリング、環境モニタリング等への応用が提案されている。920MHz帯無線マルチホップネットワークは、920MHz帯無線装置（ノード）によって自律的に形成されるネットワークであり、多数のノードが地理的に分散して配置される。このようなネットワークでは、ネットワークやノードの遠隔管理機能が重要になる。

ネットワークやノードの遠隔管理機能の一つに、ソフトウエアの更新機能がある。例えば、構造物のヘルスモニタリングなど、運用期間が長いシステムの保守管理には、作業員が各ノードを回収することなく、遠隔地から無線通信を利用してソフトウエアを更新する機能が重要になる。ここで、無線通信を利用したソフトウエア更新の問題の一つに、ソフトウエア更新データの認証がある。ノードが不正なソフトウエアを受け入れてしまうと、ネットワークシステム全体の健全性を保障できない。ソフトウエア更新などの同報データの正当性を確認する技術としては、データの完全性と配布元を認証できるデジタル署名技術がある。ただし、デジタル署名の検証には、公開鍵暗号、ハッシュ関数、多倍長演算プログラム、といった署名検証用のアルゴリズムをノードに搭載する必要がある。一方、920MHz帯無線装置が、通信データの暗号化や認証に利用する共通鍵暗号のみを利用して同報データの完全性と配布元を認証できる方式も提案されている[1)、2)]。

本稿では、920MHz帯無線マルチホップネットワークにおけるソフトウエア更新データの認証手法として、共通鍵暗号に基づくデータ認証手法を提案し、デジタル署名技術に対する優位性を述べる。

更新データ配信方法とセキュリティー条件

ソフトウエアの遠隔更新を安全に実施するためには、ノードが受信した更新データを管理サーバーからの正当なデータであると認証する必要がある。

管理サーバーが個々のノードに対してソフトウエア更新データをユニキャストで配送する場合には、更新データを配送する管理サーバーと個々のノードとが事前に一対のペアワイズ鍵を共有しておくことで、各ノードは更新データが管理サーバーからの正当なデータであることを認証できる。しかし、多数のノードで形成されるマルチホップ型のネットワークにおいては、更新データのユニキャスト配送が、通信量を増大させることになる。ここで効率的に更新データを配布するためには、ソフトウエア更新対象となるノードグループのすべてのノードが認証できる更新データを生成し、配布できるのが好ましい。例えば、マルチホップネットワークにおける効率の良いソフトウエア配布手法として、マルチホップ通信の各中継ノードが、中継先のノードに対して、管理サーバーに代わって更新データを配布する手法が提案されている[3)、4)]。しかし、更新データの認証に共通鍵暗号を利用する場合には、管理サーバーおよびソフトウエア更新対象となるノードグループに同一の認証鍵を共有させるため、グループ内の攻撃者が管理サーバーへなりすまして不正な更新データを投入することが可能である。

そこで、我々は、ソフトウエアの遠隔更新におけるセキュリティー条件として、以下の条件を満たすことを目的とした。

- マルチホップネットワークにおいて、データ送信対象となるノードグループの各ノードが、共通鍵暗号に基づいてマルチキャスト更新データの配布元を一意に認証できること。
- ノードグループ内において既に更新データを取得したノードが、管理サーバーに代わって他のノードに更新データを配布する場合でも、各ノードが、更新データのオリジナルの配布元を一意に認証できること。
- ノードグループ外に対してソフトウエア更新データを秘匿できること。

既存手法と課題

ノードグループ外に対してソフトウエア更新データを秘匿する方法として、更新データ用の鍵を、グループ内の個々のノードにセキュアに配信する方法がある。この手法では、管理サーバーと個々のノードが一対のペアワイズ鍵を事前共有しておき、管理サーバーが、更新データ用の鍵を前記ペアワイズ鍵で暗号化して対象となるノードにセキュアに通知する。管理サーバーは、更新データ用の鍵を利用して、更新データに対する認証符号を生成すると共に更新データを暗号化して配布し、各ノードは前記更新データ用の鍵を利用して、配布された更新データをセキュアに取得する。しかしながら、この手法では、更新データ用の鍵を通知された攻撃者が、他のノードに対して管理サーバーになりすますことが可能になる。 **図 1**は、本既存手法に対する管理サーバーへのなりすまし攻撃の例を示している。 **図 1**では、攻撃者が、更新グループ内の他のノードに対して、不正な更新データを、管理サーバーからの正しい更新データとして認証させることができる。

また、共通鍵暗号のみを利用したマルチキャストデータの認証手法でありながら、管理サーバーへのなりすまし攻撃に耐性を持つ手法が提案されている[1)、2)]。しかし、これらの既存方法では、データの配布元を認証するために、グループ全体が同期して認証する必要があり、前述したセキュリティー条件である、「代理配信データの配布元を一意に認証する」ことができなかった。

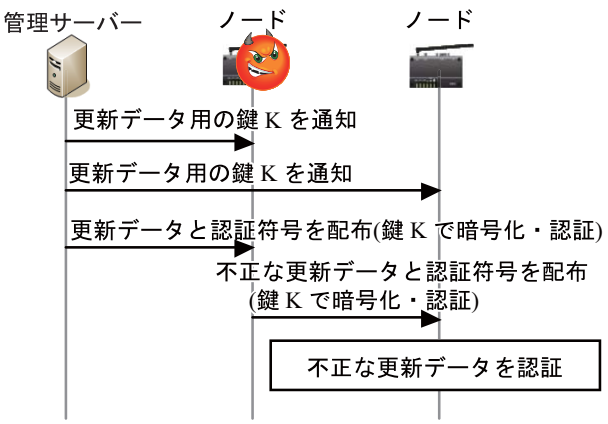

図 1　管理サーバーへのなりすまし攻撃

代理配信可能データ認証手法

本章では、共通鍵暗号のみを利用しながら、更新グループ内の他のノードからの代理配布を可能にしつつ、配布元へのなりすまし攻撃を防ぐ手法を提案する。

提案手法では、管理サーバーがノードとのペアワイズ鍵に基づくセキュアなユニキャスト通信路を利用して、マルチキャスト更新データの鍵と、マルチキャスト更新データの認証値（例えば、マルチキャスト更新データに対する認証符号またはハッシュ値）をセキュアに通知する。提案手法の動作概要を **図 2**に示す。提案手法は、次の２つのステップにより構成される。

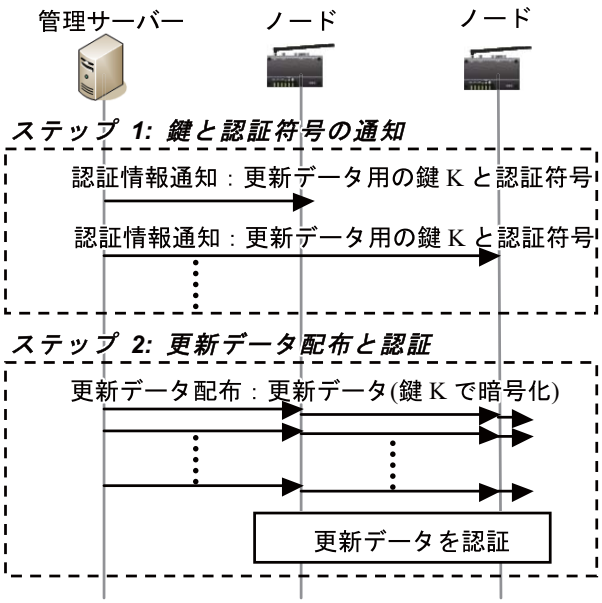

図 2　提案手法におけるマルチキャスト更新データの認証

●ステップ１：鍵と認証符号の通知

管理サーバーは、マルチキャスト更新データの配送に際し、更新データ用の鍵Kを生成し、生成した鍵Kを利用して更新データに対する認証符号を生成する。次に、管理サーバーは、更新データ用の鍵Kおよび認証符号により構成される認証情報通知メッセージを生成し、管理サーバーが確かに認証情報通知メッセージの配布元であることを各ノードに証明するために、各ノードと一対で共有するペアワイズ鍵を利用して認証情報通知メッセージを暗号化および認証符号付加し、各ノードへ配送する。

一方、各ノードは、管理サーバーと共有するペアワイズ鍵を用いて認証情報通知メッセージの復号と認証に成功することにより、マルチキャスト更新データの鍵Kおよび認証符号をセキュアに取得する。

●ステップ 2：更新データ配布と認証

管理サーバーは、更新データ配布メッセージを生成する。更新データは、数十～数百kBのサイズが想定されることから、更新データ配布メッセージは、複数の更新データ配布パケットにフラグメントされて配送されることになる。ここで、管理サーバーは、更新データを、鍵Kを利用して暗号化することでグループ外メンバーに対して更新データを秘匿する。管理サーバーは、各更新データ配布パケットをノードグループに対してマルチキャスト配送する。

ノードグループの各ノードは、各更新データ配布パケットから更新データを復元し、鍵Kで復号することにより、更新データを取得する。各ノードは、ステップ1で取得した鍵Kを用いて、取得した更新データに対する認証符号を生成し、生成した認証符号が、ステップ 1 で取得した認証符号と一致するかどうかを検証する。そして、もし一致する場合には、各ノードは、復元した更新データが、管理サーバーが配布した正当な更新データであると認証する。

さらに提案手法では、既に更新データを認証し取得した中継ノードが、管理サーバーの代わりに更新データを配布することもできる。**図 3**に、中継ノードAが管理サーバーに代わって更新データを配送する例を示す。**図 3**では、まず、既に更新データを認証し取得している中継ノードAが、自身の取得している更新データの識別情報を通知する（①更新データ通知）。ここで、自身が取得していない更新データの識別情報を通知されたノードBは、当該更新データを認証するための鍵を管理サーバーに要求し（②認証情報要求）、更新データを認証するための鍵Kおよび認証符号を、管理サーバーよりセキュアに取得する（③認証情報通知）。その後、ノードBは、中継ノードAに対して更新データの配送を要求し（④更新データ要求）、中継ノードAがノードBに対して更新データを配布する（⑤更新データ配布）。

セキュリティー考察

本章では、提案手法におけるデータ配布元へのなりすまし攻撃耐性について考察する。提案手法では、**図 2**に示すように、マルチキャスト更新データの鍵Kだけでなく、マルチキャスト更新データの認証符号をも各ノードに通知する。このように各ノードが正しい鍵Kと共に、正しい認証符号をも取得することにより、正当な鍵Kを知る攻撃者が、他のノードに不正なデータを認証させることが困難になる。なぜならば、攻撃者が、同一の認証符号を出力する不正な更新データを見つけ出すことを、計算量的に困難にできるからである。

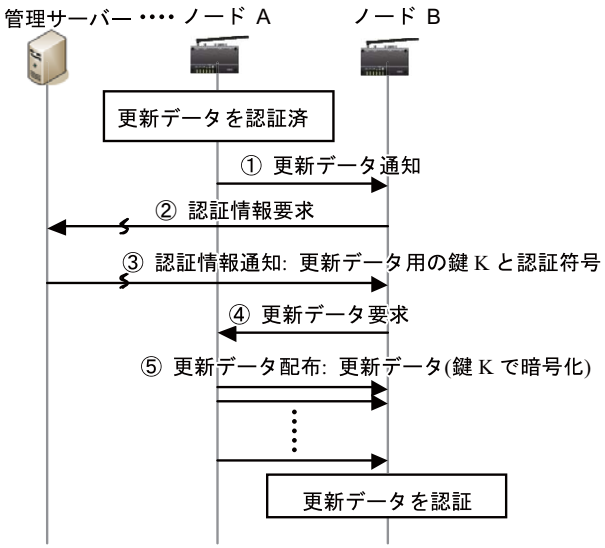

図 3　提案手法における更新データの代理配信認

デジタル署名との特徴比較

本章ではデジタル署名技術に対する提案手法の特徴を整理する。デジタル署名技術を利用してマルチキャスト更新データの配布元を認証する場合には、管理サーバーが、自身の秘密鍵を利用して生成した署名を更新データに添付し、一方、各ノードは、管理サーバーの公開鍵を利用して署名を検証する。

以下では、デジタル署名技術に対する提案手法の特徴を、ノード危殆化時の安全性、メモリー利用量、通信量の3つの観点で述べる。

（1）ノード危殆化時の安全性

デジタル署名技術では、ノードが危殆化しても、正当な署名を生成するために必要なサーバーの秘密鍵は漏洩しない。よって、攻撃者が不正なデータをノードに投入することは困難である。一方、提案手法では、ノードが危殆化し、ペアワイズ鍵が漏洩した場合には、攻撃者は、そのノードに対して不正な認証鍵と認証符号の組を投入できる。すなわち、提案手法では、ペアワイズ鍵が不正な漏洩から守られている必要があり、その前提の下で、デジタル署名技術と同レベルの安全性を確保できる。

（2）メモリー利用量

デジタル署名技術では、署名検証のためにハッシュ関数や公開鍵暗号を搭載する必要がある。例えば、

EFM32-GG390[5] 上でのデジタル署名技術のメモリー利用量を見積もったところ、256-bitのECDSA（Elliptic Curve Digital Signature Algorithm）署名検証に、約24 kBのROMを必要とした。ただし、暗号関数はOpenSSLをベースに実装しており、メモリー利用量にはECDSA署名検証に必要な楕円曲線暗号（secp256r1）、ハッシュ関数（SHA-256）および多倍長演算プログラムを含む。一方、提案手法で利用する認証符号は、共通鍵暗号のみを利用して生成できる。共通鍵暗号は、無線通信データの暗号化や認証に一般的に利用されており、例えば、32-bitのマイコンにおいて、128-bitのAES暗号は、約3 kBのROMでサポートできる。また近年は、ハードウエアAESを搭載するマイコンも多く登場している[5]。すなわち、提案手法は、920MHz帯無線装置が通常備える暗号のみで実現できると考えても良い。

（3）通信量

デジタル署名技術では、更新データにデジタル署名を添付して配布することで、各ノードが更新データの正当性を検証できる。一方、提案手法では、更新データを配布する以外に、更新データの認証情報を各ノード個別に通知する必要があるため、デジタル署名技術と比較して、通信量が大きくなる。しかし、提案手法では、グループ内の各ノードに共通の鍵を配布するため、更新データの認証だけでなく、暗号化による更新データの秘匿を同時に提供することができる。これは、更新データの認証機能しか有さないデジタル署名技術には実現できない機能である。デジタル署名技術において、ノードグループ外に更新データを秘匿する場合には、提案手法と同様にグループ内の各ノードに対する暗号鍵の事前配布が必要になる。

また、一般に、ソフトウエア更新プロトコル全体の手順を考慮した場合には、管理サーバーが各ノードに対して、ソフトウエア更新の実施通知や、更新データのサイズ等を事前に通知する必要がある。このような、ソフトウエア更新の実施に関する事前の情報通知に、提案手法に必要となる鍵や認証符号の通知を組み込むことができるため、提案手法に必要な認証情報の通知は、提案手法固有の通信量とならない。

以上、デジタル署名技術に対する提案手法の特徴を述べた。提案手法では、ペアワイズ鍵を不正な漏洩から守る必要があるものの、ソフトウエア更新手順に組み込む前提では、デジタル署名技術と比較してメモリー利用量の観点で優位性がある。

まとめ

本稿では、920MHz帯無線マルチホップネットワークの遠隔管理を目的として、代理配信可能なマルチキャスト更新データ認証手法を提案した。提案手法は、共通鍵暗号のみに基づいたマルチキャスト更新データの配布手法でありながら、グループ外への更新データの秘匿と、グループ内の他のノードからの更新データ配布を可能にしつつ、攻撃者による配布元へのなりすまし攻撃に耐性を持つ。今後の予定は、既存の920MHz帯無線装置のソフトウエア更新手順に対する提案機能の組み込みと実用に向けての性能評価である。 ◆◆

■参考文献

1） A. Perrig, et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks Journal., vol. 8, no. 5, 2002, pp. 521-534.

2） T. Yao, S. Fukunaga, and T. Nakai, “Reliable broadcast message authentication in wireless sensor networks,” LNCS, vol. 4097, 2006, pp. 271-280.

3） J. W. Hui and D. Culler, “The dynamic behavior of a data dissemination protocol the dynamic behavior of a data dissemination protocol for network programming at scale,” ACM SenSys, Baltimore, Maryland, USA, November 2004.

4） S. S. Kulkarni, et al., “MNP: Multihop network reprogramming service for sensor networks,” in IEEE ICDCS, Columbus, Ohio, USA, June 2005.

5) Energy Micro, “EFM32GG390 DATASHEET (2011-02-04 d0040_Rev0.90).”

●筆者紹介

八百健嗣：Taketsugu Yao. 研究開発センタ スマート社会ビジネスイノベーション推進部

中嶋純：Jun Nakashima. 研究開発センタ スマート社会ビジネスイノベーション推進部

福井潔：Kiyoshi Fukui. 研究開発センタ スマート社会ビジネスイノベーション推進部