センサネットワークにおけるネットワーク構成確認方式の提案とブロードキャストメッセージ認証への応用

佐藤　晃司†　　岩村　恵市†

†東京理科大学
102-0073　東京都千代田区九段北 1-14-6
sato@sec.ee.kagu.tus.ac.jp

あらまし　センサネットワークにおいて、コアノードがネットワーク構成を把握していることを前提とするプロトコルが存在する。しかし、ネットワーク構成の安全な確認方式について十分に検討されていない。本稿では、既存ルーティングプロトコルから得られた不確かなルート情報を利用し、繰り返し暗号化メッセージを用いた安全なルート情報確認方式を提案する。このメッセージは、正しいルートを通った時のみエンドノードで復号でき、復号結果から生成した受信確認をコアノードが検証することでルート情報を確認することができる。これによって、攻撃者が不正なルート情報をコアノードに申告した場合でも、センサノードの不正な利用を防ぐことができる。

Confirmation Method of Network Composition in Sensor Networks, and Application to broadcast Authentication

Sato　Koji†　　Iwamura　Keiichi†

†Tokyo　University of　Science
1-14-6 Kudankita, Chiyoda, Tokyo 102-0072, JAPAN

Abstract　The protocol to which the core node is required to know the composition of the networks beforehand exists on the sensor network. However, the method to confirm the composition of the network safely is not examined enough. In this paper, it proposes a safe route information confirmation method to use the encrypted message repeatedly by the use of uncertain route information obtained from the existing routing protocol. Only when a correct route's passing, this message can be decoded by the end node. The core node verifies the receipt acknowledgement generated from the decoding result and route information is confirmed. Illegal use of the sensor node is prevented.

1　はじめに

センサネットワークは防災、防犯、軍事などの幅広い分野で活躍が期待されているアドホックネットワークの一種である。センサネットワークでは、センサノードと呼ばれる無線通信機能とセンシング機能を合わせ持つ端末と、これに対して管理機能を持つコーディネータと呼ばれる計算機によって構成される。センサノードを多数配置し、配置されたそれぞれのノードがセ

ンシングしたデータを無線通信によってコーディネータに伝達することで情報収集などを行う。

センサネットワークで使用されるセンサノードは主に電池駆動することが想定され、電力の補充が考えられていないため、低電力化が重視されている。このため、公開鍵暗号のような大きな計算が必要な演算は困難である。さらにセンサノードは物理的に安全ではない場所に設置されることが多く、実装コストなどの問題により耐タンパ性を期待することはできない。よって、攻撃者がノードを盗難して暗号化に関するカギ情報を解析することは容易である。さらに、漏洩したカギ情報が他のノード間の暗号化通信にもちいられている場合は、ネットワーク全体が盗難の危機にさらされる危険性がある。そのため、センサノードの盗難や計算量を考慮したアルゴリズムを利用する必要である。

これに対して、コーディネータはセンサネットワーク全体の管理を行う計算機であり、センサノードでセンシングされた情報はコーディネータに集められるため、コーディネータが盗難されることは情報収集はおろか、ネットワークが機能しなくなる状況に等しい。このためコーディネータは耐タンパ性をもち、安全な場所で管理される場合が多い。またコーディネータは収集された多量の情報を処理する必要があり、演算能力は高く、メモリ容量は大きく、電源容量に制限はないことが多い。

今までのセンサネットワークに関する主な研究は、エネルギー消費を抑え効率的に通信経路を確立することが中心であった。しかし、センサネットワークのセキュリティに関する研究はあまり行われていない。特に、通信経路の確立時におけるセキュリティはほとんど研究されていない。それは、この分野の研究には、通信プロトコルとセキュリティに関する 2 つの知識が必要となるためと考えられる。

1 つの例として、センサネットワークのセキュリティについて、コーディネータがネットワーク構成を把握していることを前提とするプロトコルがいくつか存在する。しかし、センサネットワークでは事前にネットワーク構成をコーディネータが把握していることはほとんどない。実際にはハローメッセージやルート探索メッセージなどネットワークを構築するための制御情報をノード同士が自立的にやり取りを行うことでネットワークの構築が行われる。このネットワーク構築またはネットワーク構成把握は通信プロトコルに関する部分であり、その構築に関する安全性または安全な構成法の提案は少ない。

センサネットワークはアドホックネットワークの一種であり、センサネットワークにおいてもアドホックネットワークのルーティングプロトコルが利用されることが予想される。しかし、センサネットワークでは、アドホックネットワークに比べ端末を盗難、利用される可能性が非常に高く、これらを考慮し、コーディネータが安全にルート情報を収集できる仕組みが必要となる。

そこで、本論文では既存のルーティングプロトコルを利用して得られたルート情報に対して、そのルート情報が正しいかどうかを確認する方式を提案する。1 つの方法として安全性を実現する新たなルーティングプロトコルを検討することも考えられるが、ルーティングプロトコルは種々の手法が存在し、標準化されているものもあることから、既存ルーティングプロトコルから得られる情報を確認する方式を検討した。また、ルート情報を把握していることを前提として提案が行われているプロトコルとして、ブロードキャストメッセージ認証プロトコルを取り上げ、本提案方式のブロートキャストメッセージ認証プロトコルへの応用を提案する。

本論文では、2 章でセンサネットワークに適したルーティングプロトコルを検討し、3 章でルーティングプロトコルによって生成される経路表の改ざん方法を説明する。4 章では 3 章であげた攻撃に耐性のある繰返し暗号化を用いたネットワーク構成確認方式を提案する。5 章で、ルート情報を用いたブロードキャストメッセージ認証の問題点を挙げ、繰返し暗号化と組み合わせたブロードキャスト認証方式示す。

2　ルーティングプロトコル

アドホックネットワークにおいて様々なルーティングプロトコルが提案されているが、大きくリアクティブ型とプロアクティブ型に分けられ、それぞれ標準化が行われているプロトコルが存在する。リアクティブ型、プロアクティブ型の特徴を以下に示す。

・リアクティブ型プロトコル

通信要求時、初めてルート探索を行う。そのためメッセージ送信に遅延が生じる。しかし、通信要求時のみルート探索のための制御情報をやり取りするため省エネルギーである。

・プロアクティブ型

あらかじめ経路表を作成するため、通信要求時、即座に通信可能である。経路表を作成するために、定期的に制御情報のやり取りを行っており、リアクティブ型プロトコルに比べ電力の消費が激しい。

アドホックネットワークでは、頻繁な端末の移動が考慮されている。しかし、センサネットワークでは、端末の移動はほとんどなく、故障やバッテリー消耗による経路変化がほとんどであると考えられる。

よって、センサネットワークにおいて事前にネットワーク構成をコーディネータが把握するためには、制御情報をやり取りする頻度を減らしたプロアクティブ型プロトコルの利用が適していると考えられる。このプロアクティブ型プロトコルを利用することでコーディネータはネットワークの構成をあらかじめ把握することができる。

3　プロアクティブ型プロトコルを用いた際の攻撃

プロアクティブ型プロトコルには様々なプロトコルが存在するが、標準化が行われている OLSR(Optimized Link State Routing)プロトコルを取り上げ説明を行う。HELLO メッセージと TC(Topology Control)メッセージという 2 つの制御メッセージが用いられる。HELLO メッセージは周辺情報を収集するためのメッセージであり、これによって接続可能な隣接ノードを探索することができる。一方、TC メッセージは、HELLO メッセージによって収集した情報をネットワーク全体に送信するためのメッセージである。HELLO メッセージは隣接ノード間のやり取りしか行われず、転送が行われないのに対して、TC メッセージはメッセージ転送が行われ、ネットワーク全体に送信される。この TC メッセージに含まれる情報をもとに各ノードは経路表を作成していく。

しかし、これらの情報はセキュリティ情報を含まないため、攻撃者は容易に改ざんすることができる。また、センサネットワークにおいて、すべてのノードはコーディネータによって管理されるため、コーディネータの利用するルート情報はセキュリティ上非常に重要である。そのためコーディネータの得るルート情報を確認する仕組みが必要となる。

ネットワーク内の攻撃者は、HELLO メッセージで得られた情報を改ざんして TC メッセージとして送信したり、他のノードから送られてきた TC メッセージを転送しないなどすることによってコーディネータに偽のルート情報をつかませることが可能である。この時、ネットワーク内に攻撃者ノードがルート情報を改ざんする攻撃の種類として以下の 3 つがあげられる。

① ノードが存在しないにもかかわらず、存うードに接続していると偽る攻撃。
② ノードが存在しているにもかかわらず、存在していないと偽る攻撃。
③ ノードが存在しているにもかかわらず、存在していないと偽る攻撃。

①、②の攻撃が行われたルート情報をコーディネータが使用したとき、あるノードに対してメッセージを送りたいにもかかわらず、実際には存在しないノードを経由することになっている

ため通信を行うことができない。また、③の攻撃を行なった場合、攻撃者はコーディネータに知られずに存在していないと偽ったノードを利用することも可能となる。これらの攻撃はセンサネットワークへの攻撃研究[6]において、ワームホール攻撃やブラックホール攻撃、シビル攻撃などと呼ばれている。

今回、OLSR を取り上げたが、同様にプロアクティブ型プロトコルとして標準化が行われている TBRPF プロトコルにおいても、隣接ノード探索(HELLO)メッセージと、これをネットワーク全体に送信する(TOPOLOGY　UPDATE)メッセージが利用されており、上記の攻撃が行われる可能性がある。

4　ネットワーク構成確認方式

本章では、プロアクティブ型プロトコルによって得られたルート情報が正当なルートであるかどうかをコーディネータが確認する方式を提案する。

4.1　提案方式

本提案方式は、メッシュ型トポロジーによる接続を想定する。コーディネータは各ノードから送られてくる TC メッセージから経路表を作成し、図 1 のようなネットワーク構成を把握したとする。このとき、コーディネータは得られたネットワーク構成から図 1 のように分木がない一直線のルートを選択し、選択したそれぞれのルートに対して確認を行う。

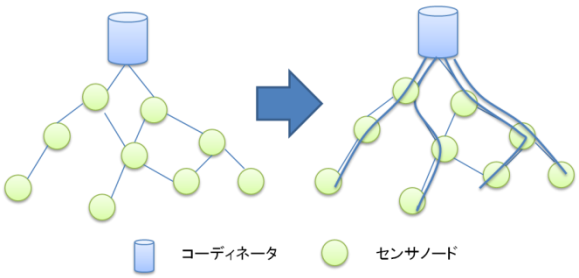

図1　コーディネータによるルート選択例

コーディネータがルート情報を確認するために、繰返し暗号化を利用したメッセージを用いる。繰返し暗号化とは 1 つの平文に対して、複数の鍵を使用し繰返し暗号化を行う暗号化方式である。これを利用すると、暗号化で使用した鍵を逆順で用いた時初めて完全な復号化が可能となる。図 2 を用いて提案方式の手順を示す。

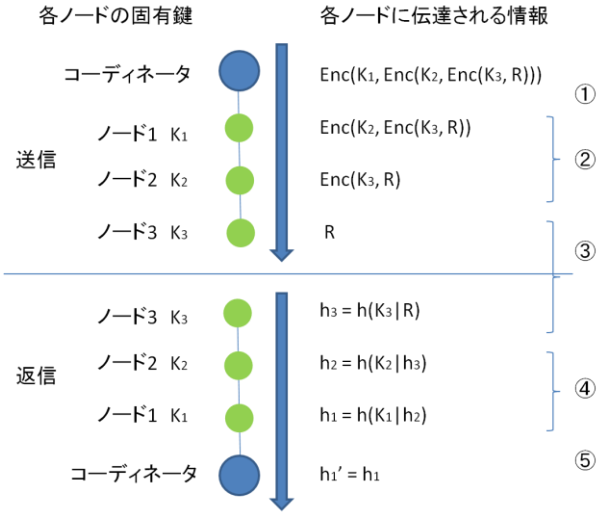

図2　ルート情報確認方式の動作図

・前提条件

各ノードは固有鍵を持つ。また、コーディネータはすべてのノードの固有鍵リストを持ちこれを自由に利用することができる。さらに、各ノードはこの確認手法を理解しており、コーディネータから下記暗号化メッセージが送られてこない時、上位ノードに不正者がいるとみなし、それ以降の通信を行わないとする。

① コーディネータは乱数を平分として、確認するルートのエンドノードで完全に復号化できるよう Enc(K1, Enc(K2, Enc(K3, R)))のように繰返し暗号化メッセージを生成する。これを使用したルート情報と一緒に送信する。

② 暗号化メッセージが送られてきたノードは自らの固有鍵を使用して暗号化メッセージを復号し、ルート情報に従って転送することを繰り返す。

③ エンドノードは繰返し暗号化メッセージが自らの固有鍵で完全に復号化が行われたことを確認し、h3 =h(K3|R)のように乱数と

固有鍵の連接のハッシュ値を受信確認としてコーディネータに返信する。

④ コーディネータまでのルート上のノードは送られてきたハッシュ値と自らの固有鍵の連接のハッシュをとり、これを転送する。

⑤ コーディネータは送られてきた受信確認 h_1 とルート情報と固有鍵リストから生成した h'_1 を比較検証し、ルートが正しいことを確認する。

4.2 提案方式の特徴

繰返し暗号化メッセージは固有鍵リストを持つコーディネータのみが生成することができ、攻撃者が不正に生成することはできない。また、正しい順番で鍵を使用しない限り復号することができないため、ノードが接続されている順番を保証することができる。また、コーディネータが受信確認を検証することで、ノードが存在しないにもかかわらず、存在していると偽る攻撃と、実際には接続していないノードと接続していると偽る攻撃を検知することができる。さらに、確認のために使用される、繰返し暗号文とハッシュ値はともに固定長の情報であり、ルート上のノード数に依存しないため、通信時のオーバーヘッドを少なく抑えることができる。

最後に、ノードが存在しているにも関わらず攻撃者によってその存在がコーディネータに申告されなかった場合、そのノードが不正に利用される恐れがあるが、制御メッセージを送信したにも関わらずコーディネータから確認メッセージが届かない場合、動作を停止することで攻撃者に不正に利用されることを防ぐことができる。

これらより、本提案方式では 3 章で示した 3 つの攻撃に対して対策が行われており、得られたルート情報が正しいことを確認することができる。

5 ブロードキャスト認証におけるルート情報改ざんによる攻撃

5.1 ブロードキャストメッセージ認証の利用

センサネットワークを利用するに当たり、センサノードの障害修復、機能変更などの際、コーディネータからのメッセージによってソフトウェアを更新できることが望ましい。これによって非常に汎用性の高いシステムを実現することができる。

このメッセージはセンサノードの動作を命令するメッセージであり、攻撃者によるなりすまし攻撃を防ぐために、確かにコーディネータからのメッセージであることを確認する必要がある。そこで、ブロードキャストメッセージ認証技術が利用される。

八百らによって、ハッシュ連鎖を用いたブロードキャストメッセージ認証方式に対して、受信確認を行うことでなりすまし攻撃に耐性を持たせた方式[1]が提案されている。ハッシュ連鎖とは、ランダムな値に一方向関数を任意回数施して生成した鍵鎖列である。この方式はコーディネータがネットワーク構成を把握していることを前提としており、もし攻撃者によってコーディネータが正しいネットワーク構成を把握していなかった場合、以下のような攻撃が可能となる。

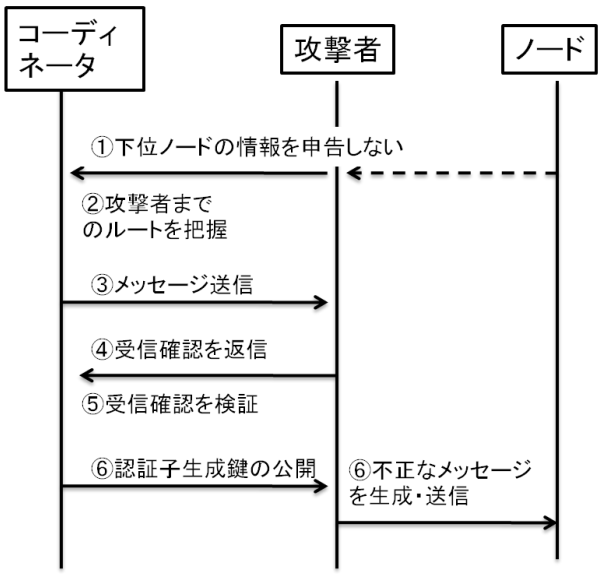

図3 ルート情報改ざんによる攻撃

5.2　ルート改ざんによる攻撃

八百らのブロードキャストメッセージ認証方式において、攻撃者は 3 章で示した、ノードが存在しているにもかかわらず存在していないと偽る攻撃を行うことで、コーディネータを偽ることが可能となる。不確かなルート情報を利用した際に想定される攻撃を図 3 に示す。

攻撃者が下位ノードの情報をコーディネータに申告しない時、実際にはネットワークに参加しているにもかかわらず、コーディネータが把握していないノードが存在することになる。すると、コーディネータは攻撃者までのルートのみを想定してメッセージと認証子を送信する。このメッセージと認証子を受信した攻撃者は下位ノードに転送せずに、コーディネータに受信確認を返信する。受信確認はコーディネータの把握したルートを経由し返信されるため、コーディネータの持つルート情報から生成した受信確認と一致し､認証子生成鍵を公開してしまう。すると攻撃者はこの鍵を利用して存在しないと偽ったノードに対して不正なメッセージを生成でき、コーディネータになりすますことが可能となる。

これに対して、前章の提案方式を行っておけば、攻撃者が申告しなかったノードはコーディネータからの暗号化メッセージが送られてこない。そのため、申告されなかったノードは上位ノードに攻撃者がいるとみなして、以降の通信を受け付けないことから、攻撃者が他ノードを不正に利用することを防ぐことができる。

6　まとめ

センサネットワークにおいて、攻撃者によるルート情報に対する攻撃方法を示し、コーディネータが不正なルート情報を利用した際の問題を示した。この問題に対して、コーディネータが得たルート情報を確認するというアプローチをとることで対策する、ネットワーク構成確認方式を提案した。また、ネットワーク構成を把握していることを前提とするプロトコルとして八百らのブロードキャストメッセージ認証プロトコルを紹介し、これに本提案方式を適用することで、攻撃者によるなりすまし攻撃を防げることを示した。

本稿で提案した方式では、繰返し暗号化を利用するために、コーディネータから一直線のルートに対して暗号化メッセージを生成する。そのため、ネットワーク構成によって効率のよいルートを選択できない場合がある。今後は、どのようなネットワーク構成においても効率よくルート情報の確認ができる方式の検討が課題となる。

参考文献

[1]八百 健嗣、松村 靖子、福永 茂”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”、 CSEC,2005, 241-246

[2]Adrian Perrig, J.D.Tygar 著、溝口 文雄 監訳”ワイヤレスネットワークにおけるブロードキャスト通信のセキュリティ”、共立出版

[3]小出　俊夫”P2P とワイヤレスの交差点”、http://internet.watch.impress.co.jp/www/column/wp2p/index.htm

[4]野田 潤、楫 勇一、中尾 敏康”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”、UBI、2008

[5]大網優太、岩村惠市、柿崎淑郎”センサネットワークにおける複数のトポロジに適用可能な鍵管理方式の提案”、IEICE、Jan.2009

[6]David Martins, Herve Guyennet”Wireless Sensor Network Attacks and Security Mechanisms”、NBiS 2010

[7] 森 郁海、森 拓海、高橋 修、” アドホックネットワークにおける攻撃法・防御法の分類と AODV ベースセキュアルーティングプロトコルの提案”、MBL 2007

[8] 佐條 研、三好 匠、” アドホックネットワークにおけるブラックホール攻撃防御法”、IEICE Technical Report CQ2007

[9]阪田　史郎、”ユビキタス技術　センサネットワーク”、オーム社