普通論文

無線センサーネットワークのためのセキュリティソリューション

デュルク ヴェストホッフ・ジョアオ ジラオ・アマルデオ シャルマ

要　旨

本稿では、無線センサーネットワーク(WSN)におけるデータ収集および処理のためのセキュリティソリューションを解説します。中規模および大規模WSN向けの適切なセキュリティ機能は、これらのネットワークを市場に向けて準備するには困難を伴いますが、欠くことのできない達成目標です。そこで本稿では、WSNのセキュリティおよび信頼性に関する課題の概要、そして、このような枠組みを支えるツールボックスのコンセプトについても紹介します。

キーワード

●無線センサーネットワーク　●セキュリティ　●揮発的環境

1. はじめに

無線センサーネットワーク(WSN)では、きわめて小型で安価なセンサーノードが使用されており、いくつかの際立った特徴を備えています。WSNは、処理電力が低くかつ無線到達距離がきわめて短いため、限定的かつ特定的なモニタリングおよび検出機能で実現する必要があります。また、領域内にある複数の無線センサーが自律的に組織化を行い、1つのWSNを形成します。感知されたデータに基づく情報は、農業や畜産、そして運転の支援だけではなく、自宅あるいは公共の場においてセキュリティを提供するために利用することもできます。技術的および商業的な視点でのキーポイントとなる必要条件は、適切なセキュリティ機能を提供することです。広範囲なサービスを提供するWSNに適したアーキテクチャが、ユーザの支持を得るためには、プライバシーとセキュリティの必要条件を満たすことが不可欠です。WSNソリューションを開発する際には、考慮すべき5つの主要な機能があります。それは、スケーラビリティ(拡張性)、セキュリティ、信頼性、自己回復機能、そして堅牢性です。これらの各機能が必要とされる度合いは、それぞれの用途によって異なります。

2. センサーネットワークの背景

2.1 テクノロジ

無線センサーネットワーク(WSN)は、ごく小規模な基地局で、あるいはまったく基地局なしで動作する特定クラスのアドホック型ネットワークを形成します。WSNは、研究および商業の両用途において、大きな可能性を秘めており、普及の兆しを見せています。センサーネットワークのノード自体は、きわめて低価格、小型の装置です。一般的に、WSNは、特定用途向けのセンサー、無線トランシーバ、汎用プロセッサで構成されますが、限定的な専用ハードウェア、さらに、周囲からエネルギーを取得するための機能やバッテリーなど、補助的な機器が含まれる場合もあります。我々は、将来想定されている用途向けに、不正開封防止機能付きのノードが入手可能となることも考慮しますが、現段階では、センサーノードが不正開封防止機能を備えることを仮定しません。

2.2 脅威モデルおよびWSNにおけるその妥当性

WSNの標準的な機能には、データの感知および収集、感知したデータの処理および伝送、そして場合によっては、データの一時的な保管、処理したデータを(いわゆる、シンクノードなどに対して)情報として提供することなどが含まれます。特に不可欠な処理(後述)としては、センサーノードにおけるデータ集約が挙げられます。このような機能をセキュアに提供することは困難ですが、重要な研究課題です。通信ネットワーク内の暗号プロトコルを系統的に分析する際には、Dolev-Yao[1]脅威モデルがよく利用されますが、WSNの分析のためのモデルとしては限界があります。

Dolev-Yao脅威モデルでは、2つの通信当事者、たとえば、A(lice)とB(ob)がセキュアではないチャンネル上で通信を行うことが想定されています。しかし、侵入者が通信ネットワーク

に対する支配権を得た場合、その侵入者は通信当事者間の通信を盗み聞きすることが可能となり、途中でその通信を傍受し、対象となる受信者への配信を妨害することも考えられます。しかし、この脅威モデルでは、終端点(AliceとBob)が自らの攻撃対象となることは想定されていません。WSNに対応する脅威モデルは、チャンネルがセキュアでないことを想定し、さらに終端点も必ずしも信頼できるものではない状況に対応する必要があります。攻撃者が、物理的にセンサーノードを盗み、機密に関わる情報の抽出を行う可能性は否定できません。

2.3 確率論的セキュリティ

前節で記述したような損害を限定的なものに留めるためには、以下に示す2種類のアプローチがあります。

1) 不正開封防止機能付き装置

重要データなど、機密情報を保存する各センサーノードに不正開封防止機能付きの装置を装備し、ノードが盗まれることに伴う損害に歯止めをかけます。

2) 確率論的セキュリティ

この設定では、センサーノードには不正開封防止機能は付いていないものと想定しており、攻撃者が盗んだセンサーノードからデータを読み取った後で取得できる情報に制限をかけることを目的としています。

最初のオプションは、コストが高くなるため、高額なコストに見合うほど重要な用途、あるいはセンサーが少なくてもすむ用途など、適用範囲が限定されます。装置に不正開封防止機能を付けられない場合、我々は、確率論的セキュリティをめざします。このアプローチでは、攻撃者がWSNから「明確に定義された」一部の知識しか取得できないことを表す「limited gain(限定的な獲得)」という用語が用いられます。

2.4 セキュリティソリューションの設計空間

一般的に、WSNを構成するノードは小型であり、その通信能力、計算能力、記憶容量、電力容量はきわめて限定的なものです。たとえば、Berkeley Motes[2]では、4KBのメモリを搭載した8ビット、4MHzのマイクロコントローラ(MCU)と最高10kbpsのデータ転送速度を持つ無線トランシーバが使用されています。大半のセンサーは、コストを抑えるために、不正開封防止機能を備えておらず、これがセキュリティに影響を及ぼしています。また、計算能力や記憶容量も限られているため、大きな数のモジュロ演算は困難であり、非対称暗号方式(公開鍵)にも不向きです。特に、古典的なDiffie-Hellman(DH)鍵交換プロトコルは除外されています。WSNのセンサーにとっては、Rivest、Shamir、Adleman(RSA)方式の小さな数の指数版でさえも、きわめて高価なものとなってしまいます。つまり、プロセッサ集約的な作業を必要としない、きわめて低コストな方式みが必要とされています。また、1ビットを送信するには、プロセッサ命令を1つ実行するよりも、およそ10^2倍もコストがかかります。送信するデータを減らすには、データ集約を利用して、ノードにおいてデータ(値)を結合します。

3. 主要な研究領域

セキュアで信頼性の高いWSNを開発するために、主要な研究領域を「セキュリティと信頼性」、「ルーティングと転送」そして「ネットワーク内処理」の3つに分類しました(**図1**)。まず考慮すべきソリューションは、確率論的セキュリティを目的とする拡張Dolev-Yaoモデルです。

上記の研究領域のうち、上位十位以内に挙げられた関連研究課題は以下のとおりです。

1) 柔軟なルーティングおよび集約ノードの選択

設定済みのWSNは、徐々に、あるいは急激に消滅するノードに十分対処できる柔軟性を備えている必要があります。全体的な方式としては、ルーティングおよび複数レベルの

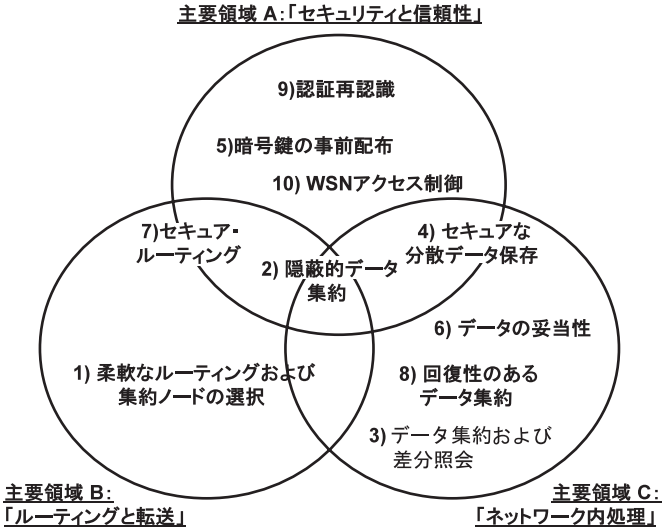

図1　主要な研究領域

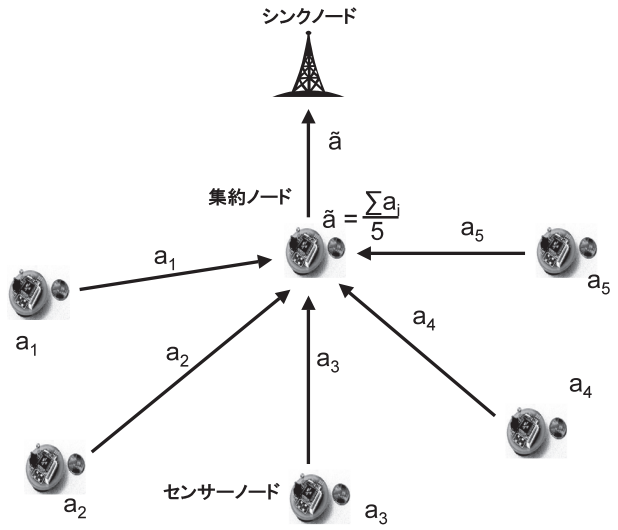

図2　ネットワーク内処理と
リバース・マルチキャスト・トラフィック

ネットワーク内処理をサポートする必要があります。**図2**は、単一レベルのの集約ノードを1つ備えたWSNの典型的なトラフィック･パターンを示したものです。この場合、集約ノードで実行される集約関数は「平均」です。大規模なWSNでは、複数の集約ノードと複数レベルの集約ノードが使用されます。集約ノードの再選択は､WSNにおけるエネルギー消費のバランスを保つのに有効です。

2) 隠蔽的データ集約

センサーノードにおけるエネルギー消費およびノードに対する物理的な攻撃による影響の両方を低減することは、WSNにおいて重要課題です。この問題に対処するために､「リバース・マルチキャスト・トラフィック」とも呼ばれる、センサーからシンクに至るエンド・エンド間の暗号化のための高度な仕組みが利用されています。隠蔽的データ集約は､センサーノードにおけるデータ処理を可能にするとともに、エネルギー効率とセキュリティの優れたバランスを提供します。図2に示された集約ノードは、暗号化されたデータを集約できるノードである必要があります。

3) データ集約および差分照会

モニターされたデータの圧縮表現および転送を行うには、1つのメッセージで複数の種類の値(たとえば、気温と湿度)を送信する方法が有効です。この手法は、送信するデータ量を抑制できるため、定義済みの差分値のみを送信する場合においても役立つ場合があります。

4) セキュアな分散データ保存

いくつかの用途においては、モニターされたデータを分散して保存する必要があります。権限を持つ照会相手に対して、揮発性の地域情報をリアルタイムで転送するのが望ましくない､あるいは､不可能な場合は､WSN自体が､モニターしたデータを保存する必要があります｡WSNは、時間の経過によってノードが消滅するという非持久的な環境であるため、セキュリティに加えて、スペースおよびエネルギー効率の良い記憶装置を考慮に入れた複製という手段を用意する必要があります。

5) 暗号鍵の事前配布

WSNが稼働を開始する前に、製造メーカが、暗号鍵などの機密情報をすべて設定することは不可能です。また、一部の機密情報については､ネットワーク･トポロジー内のノードの最終位置を把握しない限り、決定、保存することはできません。暗号鍵を配布する際に考慮すべきもう1つの要素としては、トラフィック・パターン(データがネットワーク内をどのように流れるのか)が挙げられます。

6) データの妥当性

一部の用途においては、シンクノードで受信されたデータ、そして、集約されたデータの妥当性を検証する必要があります。妥当性の検証には､冗長な情報が不可欠であるため、正確性と効率性の妥協点を求める必要があります。また、妥当性の検証においては、それぞれのWSN適用業務の意味論も考慮する必要があります。ソリューションごとに、WSNの特定のポイントにおける、依存性、および、正確性と効率性の適切な妥協点を調べることが必要です。

7)セキュア・ルーティング

ルーティングは、マルチホップのセンサーネットワークにおける、最も基本的なネットワーク機能の1つです。悪意のあるノードの存在を考慮に入れ、予防策を講じる必要があります。ルーティングには、シンクノードへの経路を見つけ、その経路を経由してデータパケットを転送するという、2つの主要な機能があります。ルーティング・プロトコルのためのセキュリティアプローチは、主に系統的ではない手段による分析のみでした。セキュリティを正確に定義することの可能な数学的枠組みが必要とされています。

8) 回復弾力性の高いデータの集約

ここでは、入力データの改ざんをたくらむ敵対者の存在を考慮し、ノードにおけるデータ集約の堅牢性や回復性を向

上させる方法について考えます。ソリューションは、シンク、センサーの両ノードにおけるデータ集約に対応する必要があります。どのようなソリューションにおいても、ある程度の割合で偽陰性が発生することを考慮に入れ、その偽陰性を受け入れる必要があります。

9) ペアワイズ/グループワイズ認証

一般的に、ノードは、事前に準備された機密の、あるいは共通のセキュリティ・インフラストラクチャなしで、明確に定義されたセキュリティアソシエーションを確立することが必要です。この場合は、一対の主体が、ペアワイズの関係を確立します。また、主体のグループが新たな関係を確立できるようにするという方法も考えられます。どちらの認証、あるいは再認証方式を採用する場合でも、エネルギー消費や記憶装置といった必要条件を考慮に入れる必要があります。

10) WSNアクセス制御

許可された当事者のみがモニターされたデータにアクセスできるようにするためには、WSNアプリケーションのエンドユーザに対するアクセス制御を提供することが不可欠です。センサーのバッテリー消費を抑えるために、使い勝手の良いデータ照会方法やDoS攻撃に対する反応性もサポートする必要があります。

4. UBISEC&SENSプロジェクト

EU特定目標研究プロジェクト(European Specific Target Research Project:STReP)のUbiSec&Sens、「Ubiquitous Security and Sensing in the European Homeland」(2006年1月～2008年12月)は、第3章で分類されている研究領域、一連のWSN適用アプリケーションおよびシナリオ(農業、交通、国土安全保障)のためのセキュリティ・アーキテクチャーを提供することを目的としています。このプロジェクトは、**図3**で示される、セキュリティ対応コンポーネントのツールボックス化を目指しています。このツールボックスは、将来登場する無線センサーネットワーク適用業務向けのセキュリティサポートを開発する際の、製造メーカ、サービス開発者による構築を容易にします。このプロジェクトは、以下の研究領域のための確率論的セキュリティの実例に続くものです。

4.1 認証と再認証

WSNにおける最大の脅威の1つが、ネットワーク内に偽装

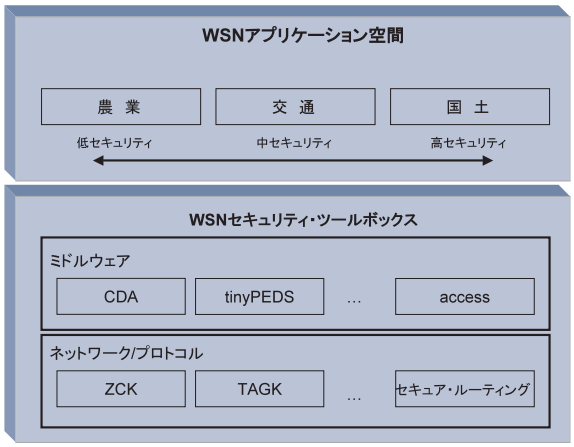

図3　UbiSec&Sensのツールボックスのコンセプト

データを侵入させたり、集約ノードに成りすます敵対者の存在です。現在、認証のための仕組みは、公開鍵暗号方式などの複雑な計算に基づいていますが、これはWSNには適用できません。大多数のシナリオにおいては、共有暗号鍵を発行する権限者は用意されておらず、分散的に通信を行う手法が用いられる傾向があります。我々は、共通のセキュリティ・インフラストラクチャや暗号鍵の事前共有を利用せず、Zero Common Knowledge(ZCK)プロトコル[2]によって、主体間に明確に定義されたペアワイズのセキュリティアソシエーションを確立する認証プロトコルを提供します。一対の通信ペアごとに2つのキーによるハッシュチェーンを用いることにより、システム内で一定レベルの信頼性を構築することができます。なお、ZCKでは、通信相手の再認証も保証されています。

4.2 隠ぺい的データ集約

Concealed Data Aggregation (CDA)[3] のアプローチでは、モニタリングを行っているセンサーノードとシンクノード間のリバース・マルチキャスト・トラフィック用に、検出されたデータの終端間暗号化を行う際、symmetric additively homomorphic encryption transformations (対称付加的同形暗号化変換)の使用を提案しています。CDAは、中間にある集約ノードに、メッセージの暗号解読と再暗号化の負担を強いることなく、暗号を集約することを可能とします。これらの集約ノードには、機密事項である暗号鍵を保存する必要はありません。CDAのサポートする集約は、homomorphic encryption transformations(同形暗号化変換)に基づいており、平均、移動感知および分散など

の関数が含まれます。文献5)では、order preserving encryption scheme(順序付け維持暗号化方式)をどのように利用して、暗号化されたデータの比較を行い、感知された最小値および最大値を含むように一連の集約関数を拡張しているのかを示しています。我々は、この方式をセンサーノードに実装しました。

4.3 KPS:Key Pre-distribution(暗号鍵の事前配布)

暗号鍵の事前配布の問題、および主要なトラフィック・パターンである「リバース・マルチキャスト・トラフィック」への対応については、Topology Aware Group Keying (TAGK:トポロジー対応のグループ暗号鍵)を紹介している文献3)に言及されています。WSN起動時および最初のブートストラップの段階で、利用可能なすべてのノードは完全な自律的組織化を行い、トポロジーに対応した方法で隣接するノードを見つけ出し、それぞれの役割を把握します。TAGKは、時間および領域ごとにランダムに選択されたグループの暗号鍵を使用して、リバース・マルチキャスト・トラフィックのために、相互には交わらない領域を確立します。TAGKは確率論的セキュリティを提供し、CDAを利用可能にするためには不可欠です。我々は、きわめて大規模なWSNのシミュレーションを行い、このアプローチの実行可能性とスケーラビリティを確認し、さらに、この方式の実装も完了しています。

4.4 セキュアな分散データ保存

現在、我々は、WSNにおいて暗号化されたデータを連携保存するという、分散データベースと同様の手法を模索しています。センサーネットワークの用途のうち、非同期的で、シンクノードに対する接続が一時的なものについては、ノードは、一定期間にわたってモニターされた周囲のデータの集約、保存を行い、以後の照会要求に対応できるものでなければなりません。また、敵対者が、ノードに保存された機密にかかわるデータを一切入手できないよう留意する必要もあります。永続的暗号化データ保存(tinyPEDS、Persistent Encrypted Data Storage)のアプローチ[6]では、長期にわたるデータ保存を目的とした集約機能を用いて、(実際の)非同期付加的同形暗号化変換 (asymmetric additively homomorphic encryption transformation)[7]を適用することにより、モニターしたデータをネットワーク内に保存する際の信頼性とセキュリティを高めるアーキテクチャを提案しています。tinyPEDSでは、保存された値を取り出す照会プロセスに加えて、ネットワークの大部分が突然消滅するというシナリオに基づいて、災害によって影響を受けた値を復旧する仕組みも提供されています。tinyPEDSは、我々のシミュレーションによる検証の対象でしたが、現在は、センサー・プラットホームへの実装の段階を迎えています。UbiSec&Sensソリューションについては、農業および交通サービスという、代表的な無線センサーのアプリケーションに基づくシナリオが用意され、試作と検証が行われる予定です。http://www.ist-ubisecsens.orgを参照下さい。

5. おわりに

以上、WSNのセキュリティと信頼性に関する課題を説明してきました。我々は、STReP UbiSec&Sens* において、モジュール式のツールボックスの開発をめざし、中規模および大規模なWSN向けに統合化されたセキュリティと信頼性を備えたアーキテクチャをサポートするという目的を実現するために、3つの補完的なWSN適用業務の分析を行っています。

* 本稿で紹介されている研究は、部分的に、EU Framework Program 6 for Research and Development (IST-2004-2.4.3) のSTReP UbiSec&Sens内にあるEuropean Commissionによって支援されています。本稿に掲載されている見解および結論は執筆者によるものであり、必ずしもUbiSec&SensプロジェクトまたはEuropean Commissionによって表明、あるいは黙示された公式の方針や支持を意味するものではありません。

参考文献

1) D. Dolev, A.C. Yao, On the security of Public-Key Protocols, IEEE Transactions on Information Theory, 29(2):198-208, 1983年
2) A. Weimerskirch, D. Westhoff: Zero-Common Knowledge Authentication for Pervasive Networks, 10th Selected Areas in Cryptography, SAC'03, Springer-Verlag LNCS 3006, pp. 73-87, カナダ, オンタリオ州, オタワ, 2003年8月
3) D. Westhoff, J. Girao, M. Acharya: Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution and Routing Adaptation, IEEE Transactions on Mobile Computing, 2006年
4) M. Acharya, J. Girao, D. Westhoff: Secure Comparison of Encrypted Data in Wireless Sensor Networks, 3rd WiOpt, 2005年4月
5) J. Girao, D. Westhoff, E. Mykletun, T. Araki: TinyPEDS: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks, Accepted for publication at Elsevier AD HOC Networks Journal.
6) E. Mykletun, J. Girao, D. Westhoff Re-visited: Public key based cryptoschemes for data concealment in wireless sensor networks, IEEE ICC, トルコ, 2006年5月

執筆者プロフィール

デュルク ヴェストホッフ
Chief Researcher,
The Mobile Internet Group,
R&D Network Laboratories,
NEC Europe Ltd.
Member of the IEEE

アマルデオ シャルマ
Manager, The Mobile Internet Group,
R&D Network Laboratories,
NEC Europe Ltd.
Senior member of the IEEE

ジョアオ ジラオ
Researcher, The Mobile Internet Group,
R&D Network Laboratories,
NEC Europe Ltd.
Member of the IEEE and the ACM