3-12 センサ・アドホックネットワークにおけるノード間のセキュリティポリシを用いた自律的アクセス制御

3-12 Autonomous Access Control among Nodes in Sensor Networks with Security Policies

岩尾忠重　雨宮真人
IWAO Tadashige and AMAMIYA Makoto

要旨

本稿ではセンサネットワークのポリシ制御の新しい枠組みについて述べる。センサネットワークには、多くのノードがあり、それらノードは様々なアプリケーションで共有される。したがって、センサネットワークでは、各ノードが様々なアプリケーションを受け入れ、かつ、容易にノードにアプリケーションモジュールを配備する能力を持つ必要がある。また、このとき各センサノードには、アプリケーションに応じた適切なモジュールが配置されるべきである。VPC on KODAMA に基づく本枠組みは、センサノードがポリシで割り当て規則により適切なモジュールを持つことを可能にする。ユーザがアプリケーションポリシをセンサネットワークの一つのノードに渡すだけで、センサノードは、そのポリシを伝播し、各ノードでのアプリケーションにおける適切な役割を実行する。また、ポリシによりセンサネットワークがアクティブ RFID の ID に応じて動的に振る舞いを変えることを例として示す。

This paper describes a new framework of policy control sensor networks. Sensor networks are shared by various applications, and have many nodes. Hence, sensor networks need to have ability to accept various applications, and to deploy application modules to nodes easily. Sensor nodes should have appropriate application modules. A framework that is based on VPC on KODAMA enables sensor nodes to have appropriate modules by assignment rules in a policy. When users only put application policies to sensor networks, sensor nodes propagate the policies and perform appropriate roles in the applications. This paper also shows that sensor networks with policies change behavior corresponding to detected active RFID tags as an example.

[キーワード]
センサネットワーク，アドホックネットワーク，ポリシ，アクセス制御，RFID，マルチエージェントシステム
Sensor network, Ad-hoc network, Policy, Access control, RFID, Multi-agents systems

1　まえがき

センサネットワーク[1][2]は、ユビキタス環境を実現する重要な要素の一つとして期待されている。センサネットワークは物理的な世界と論理的な世界をつなぐ架け橋であり、物理現象を感知し、それを論理的オブジェクトに変換し、論理世界での相互作用の結果として物理現象としてフィードバックする。ユビキタス環境の入口として重要な役割を持つセンサネットワークは、温度や、加速度や、GPS による位置や、赤外線などの様々な物を感知する。また、センサネットワークは物理的な現象だけではなく、RFID などの人工の物も扱う。RFID タグはセン

サネットワークが観察する物の一つである。RFID タグは、人々と商品を管理する場合に使用される。

近い将来センサネットワークを使用する多くのアプリケーションが現れると考えられる。人々は、センサネットワークを使用することで様々なサービスを得ることができる。このとき人々は同じセンサネットワークを共有し、そして、多くのアプリケーションが同一センサネットワーク上に動作することになる。そのような状況においては、センサネットワークは、ユーザが様々な目的に使用することができる必要がある。また、各ノードへのアプリケーションの展開は簡単であるべきである。アプリケーションはダイナミックにインストールされるべきであり、また、適切なモジュールが適切なノードにインストールされるべきである。しかしながら、センサネットでは、ノードの数が非常に多くなるため、人の手によってモジュールを各ノードにインストールするのは難しい。適切なモジュールが自動的に適切なノードにインストールされる方法が必要である。また、セキュリティも重要な問題である。センサネットワークが個人的なデータを扱うとき、そのデータは保護されるべきである。センサネットワークが画一的なセキュリティの手法でデータを扱うことは十分でない。例えば、アプリケーションによっては、検知データに応じて、それぞれ異なる認証を必要とするノードを通過する必要があるかもしれない。このような場合、アプリケーションに従ってデータを扱う安全な方法が必要である。したがって、センサネットワークには、アプリケーションモジュールを適切にノードに配備し、安全にデータを扱い、動的に様々なアプリケーションをサポートする枠組みが必要である。

我々は、センサネットワークの新しい枠組みを提案する。この枠組みは、ポリシを用いてマルチエージェントシステムを制御することを可能とする VPC on KODAMA[3]-[6]をベースとしている。エージェントはポリシに基づきコミュニティを構築する。ポリシはコミュニティにエージェントが入るための条件及びコミュニティの中でのエージェントの役割について定義する。ポリシは役割の割付ルールを含んでいる。エージェントの属性と割り当てルールに従って、役割はエージェントに割り当てられる。エージェントは、割り当てられた役割に従って行動して、互いと協力することによって、サービスを提供する。VPC on KODAMA のエージェントは、他のエージェントを認証して、安全に役割を割り当てるための機能を持つ。センサネットワークでは、エージェントはセンサノードである、そして、役割はデータの検出及びそのデータの処理である。VPC on KODAMA をセンサネットワークに適用することによって、センサネットワークは、アプリケーションポリシを受け入れて、各ノードに適切なモジュールを配備して、安全にデータを処理することができる。

2 はポリシによる多目的のセンサネットワークのコントロールについて述べる。センサネットワークにおける VPC on KODAMA は **3** で説明する。この枠組みを用いた例を **4** で示す。例として、検出された RFID とポリシによりセンサネットワークは振舞いを変える。**5** では関連研究について述べる。

2 多目的センサネットワークにおけるポリシ

2.1 多目的センサネットワークの要件

センサネットワークでは、多くのセンサノードが物理現象を検出し、その検出データを処理して、互いに通信する特徴がある。多目的のセンサネットワークでは、各センサノードを様々なアプリケーションで使用することになる。

各ノードには、様々なアプリケーションをサポートするための何らかの枠組みが必要である。多目的のセンサネットワークでサービスを実行するために、それぞれのノードは様々なアプリケーションを受け入れることができるべきである。すべてのアプリケーションモジュールがあらかじめセンサノードにあるというのは現実的でないため、センサノードは動的にアプリケーションの受入れを可能とするべきである。また、センサネットワークのノード数は膨大になることが予想されるため、人の手でアプリケーションを各ノードにインストールするのは難しい。

センサネットワークが扱う個人の情報を使う場合、セキュリティが重要となる。個人情報データはセンサネットワークで保護されるべきである。検知データによって、保護の仕方は変化するかもしれない。アプリケーションごとに異なるセキュリティの制御機構を取り入れることができる機能を多目的センサネットワークの枠組みは持つべきである。このように、多目的のセンサネットワークに、重要な要素は、アプリケーションの多様性とその展開及びセキュリティである。

● アプリケーションの多様性

センサネットワークにおけるアプリケーションは多くのセンサノードが互いに協調しサービスを提供する。それぞれのセンサノードは、それ自身の役割を持って、その役割を実行する。アプリケーションは、それぞれのノードの役割の協調によるものである。幾つかのノードの役割は他のノードと異なっているかもしれない。ある役割は、認証されたノードのみが実行できるタスクかもしれない。このようにセンサネットワークにおけるノードの役割は同じでない。適切な役割は適切なノードに割り当てられるべきである。

● アプリケーションの配置

アプリケーションをセンサネットワークに配置するとき、二つの問題がある。一つは、センサノードの数であり、アプリケーションをセンサネットワークにインストールするとき問題となる。また、別の問題はインストールモジュールが他のモジュールと異なっているということである。両方の問題を解決するために、数の多いセンサノードでの各ノードには適切なモジュールが自動的にあるのを可能にするメカニズムが必要である。

● 安全性

センサネットワークにはセキュリティに関する重要な二つの点がある。それは、検知データの保護とセンサネットワークの保護である。検知データの保護はセンサネットワークがどう安全に検知データを扱うかということである。センサネットワークの保護はセンサネットワークが不法なデータとアクセスからどうそれ自身を守るかということである。センサネットワークの処理は、データを検出し、処理し、そして転送することである。それぞれの過程において、二つの視点のセキュリティを考える必要がある。

最初はノードがあるデータを検出するシーンである。センサノードが、検出されたデータが本物であるかどうか検出することができるなら、センサノードは、そのようなメカニズムを持つべきである。しかしながら、一般に、温度や湿度などの物理的な現象を、本物かどうかをはっきりさせるのは難しい。このような場合は、複数のセンサの結果を照らし合わせて判断することになる。また、データがバーコードや RFID などのように人工物であるなら、センサノードはそれらをはっきりさせる電子署名などのメカニズムを持つことができる。メカニズムがアプリケーションによるので、この場面にも、ダイナミックにモジュールを得る能力は有効である。

次は、ノードが検知データを処理する場面である。上の議論より、処理モジュールは外部から導入されることが望まれる。この場合、処理モジュールの認証が必要である。処理モジュールは処理データが不法なデータであってもうまく振る舞うべきである。例えば、RFID の ID を検出した場合、それが不正な場合、破棄する必要がある。RFID の ID が不正かどうかはシステムに依存し、不正時の処理はそれぞれアプリケーションの処理モジュールに依存する。

最後は、ノードが処理データを他のノードに送る場面である。この場面では、ノードは、データを送ろうとする、もしくは受け取ろうとするノードが信用できるかどうか決めなければならない。アプリケーションはセンサネットワークにすべてのノードを使用するというわけではない。アプリケーションへの関連するノードだけが、データを互いから送るか、又は受取ることができるべきである。その意味では、我々はアプリケーションによって、論理的なネットワークが異なっていると考えることができる。論理的なネットワークがそれぞれアプリケーションにあるとする場合、あるアプリケーションのノードは、送出・受信するノードがそのアプリケーションの論理的なネットワークに参加するなら、データを送るか、又は受け取ることができる。重要なポイントはアプリケーションへの

関連するノードがどのようにアプリケーションの信用の論理的なネットワークを構築するかということである。センサネットワークには中心となるノードはない。したがって、アプリケーションへの対応するノードは、特別に自主的に論理的なネットワークを創設する必要がある。

2.2 多目的センサネットワークにおけるポリシ制御

大規模な数のノードを制御するためにはポリシによる制御は人間社会における法と同様に効果的な方法の一つである。大規模な数のノードにおいて、一つ一つのノードを人間の手によって直接制御するのは難しい。法のようなものに従って、ノードは自分たちで自主的に制御されるべきである。私たちはここにそのような各ノードが従う記述、をポリシと呼ぶ。

多目的のセンサネットワークにおけるポリシは、これまでの議論より以下の点が重要である。

(1) どのように適切なノードに適切な役割を割り当てることができるか。
(2) センサネットワークにおける役割は、センサのためのスキーマとアドホックネットワークのためのスキーマがある。センサスキーマはセンサノードがどうデータを検出して、処理するかということである。アドホックネットワークスキーマは、いかにアプリケーションごとの論理的なネットワークを作成し、ノードがデータをどう転送するか、又はどう受け取るかということである。
(3) 各ノードは、与えられたポリシが本物であるかをどう知るか。

多目的のセンサネットワークのための枠組みは、ポリシ制御のために上の三つの項目をサポートするメカニズムを持つべきである。

3 アドホックネットワークにおけるポリシを用いたルーティングとアクセス制御

3.1 VPC on KODAMA

VPC on KODAMA[3]-[6]はポリシでマルチエージェントシステムを制御するメカニズムを提供する。エージェントは、本物のポリシを検出して、それらの属性と割り当てルールに従って、それら自身の役割を決めることができる。

VPC on KODAMA の構造にはコミュニティの階層構造がある。エージェントは、コミュニティに所属しており、また、自分たちにそれら自身のコミュニティを持つ。エージェントには、二つのポリシと属性がある。一つのポリシは、エージェントがコミュニティに入るための条件及びそのコミュニティの中の役割について定義した公共のポリシである。別の方針は属性などの自己のプライベートなデータにアクセスするための条件について定義するプライベートなポリシである。

エージェントがコミュニティのポリシの条件を満たすとき、エージェントは、コミュニティに参加することができ、そのポリシに従いコミュニティの中での役割を持つことができる。図1にパブリックポリシの構造を示す。役割を持つための条件はエージェントに対応する属性があるかどうかということである。パブリックポリシには、エージェント自身の電子署名があり、他のエージェントは、署名を確認することにより、ポリシが本物であるかどうかを確認することができる。

役割の決定は、耐タンパデバイスを用いる。耐タンパデバイスとは、情報不正取得や改ざんに対して耐性のあるデバイスである。エージェントの属性は耐タンパデバイスに格納される。そのため、ユーザさえ属性を不正に変更することができない。各エージェントは、PKI 証明書などのそれ自身の属性を持つ。ポリシによる属性と条件に従って役割を決定するモジュールは耐タンパデバイスにある。エージェントは、ポ

```
<policy package>  ::=   <rules> <roles> <contents>
          <rules>  ::=   <rule> | <rule> <rules>
           <rule>  ::=   <condition> <role names>
     <role names>  ::=   <role name>
                   |     <role name> <role names>
      <condition>  ::=   "TRUE"
                   |     "and" <condition> <condition>
                   |     "not" <condition>
                   |     "eq" <attribute>
      <attribute>  ::=   <variable name> <value>
      <attribute>   |    <db name> <key ID> <serial number>
          <roles>  ::=   <role> | <role> <roles>
           <role>  ::=   <role name> <modules>   <init description>
       <contents>  ::=   <content> | <content> <contents>
        <content>  ::=   <content name> <content path>
```

図1 パブリックポリシの構造

リシの署名をチェックして、条件を耐タンパデバイスにある決断モジュールに送って、コミュニティ内のそれら自身の役割を得る。ここではコミュニティの役割はプログラムモジュールとして実装されている。エージェントは、役割に対応するプログラムモジュールを読み込み、モジュールを実行する。

3.2 動的なネットワークの構築

アドホックネットワーク[7][8]は、動的にノードの追加、削除しても通信を継続することを可能とする。アドホックネットワークにおけるノードは、目的ノードに送るのに適切な隣接ノードを選択し、受信データの転送を繰り返す。この結果、幾つかのノードを経由してデータを転送することが一つの特徴である。ノードは、目的ノードへの経路を作成し、データを転送する能力があるエージェントである。これらのネットワークは、ユーザが容易にセンサノードを配備するのを可能にする。

アドホックネットワークでは、以下の機能が重要である。

(1) 経路の発見
(2) データ転送
(3) リンクの維持

経路の発見は、二つのノードの間の適切な通信経路を見つけることである。データ転送はノードがどうデータを他のノードに転送するかということである。リンクの維持はノードがルーティング経路の隣接ノードと通信可能であるかどうかをチェックすることである。隣接ノードが交信することができないなら、ノードは、別

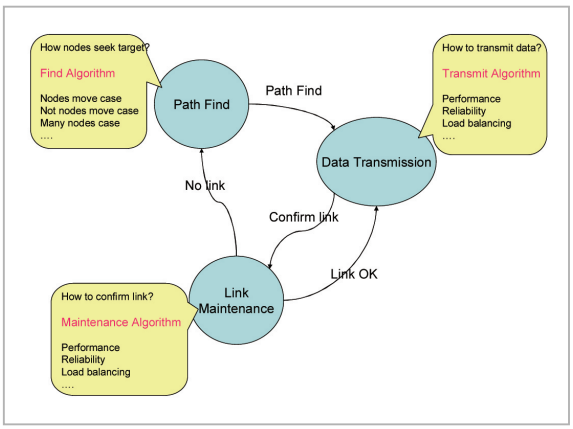

図2 アドホックネットワークの機能の関係

のルートを見つける必要がある。これらの機能の関係は図2に示す。

はじめに、通信ノードは、目標ノードへのルーティング経路を見つける必要がある。ルーティング経路の発見により、ノードは目標ノードに送り届けるための隣接ノードを知ることができる。ノードは、隣接ノードが利用可能である間、データを隣接ノードに送ることによって、データを目標ノードに送ることができる。ノードは、隣接ノードの移動や機能不全が起こることも考慮し、隣接ノードが利用可能であるかどうかチェックする必要がある。隣接ノードが利用不能であることを検出したとき、ノードは別の経路を見つける必要がある。その後に、ノードは同じルーチンを繰り返す。

アプリケーションとノードの状況によって、これらの機能の実現は異なる。ノードが重要なデータを扱うなら、ノードはデータを転送するのに信頼できる方法を取るべきである。ノードはアプリケーションが転送性能に関係があるとき、信頼性よりむしろ転送性能に重点を置いた方法を取るべきである。また、データ伝送方法も物理現象のデータと個人的なデータとで異なっているべきである。個人的なデータは、安全な状態で転送するべきである。

このように、これらの機能を実現するためのアルゴリズムはアプリケーションに応じて適切なものを選択すべきある。すべてのアプリケーションに対応したアルゴリズムをはじめから持つことは困難であるため、ノードは、外部から適切なアルゴリズムを実装したモジュールを受け入れる能力を持つべきである。

また、アルゴリズムはネットワークとしての振舞いであると考えられるべきである。巨視的なネットワークの視点では、全体のネットワークとしての振舞いは重要な問題である。各ノードがうまく動作しているように思えても、ネットワークとして動作しないのは意味がない。ネットワークのトラフィックがネットワークの許容量を超えても、アドホックネットワークは安定しているべきである。全体のネットワークとして振舞いは、個々のノードの状態コントロールと機能が決定する。例えば、複数のノードが一つのメディアを共有しているため、多くのノ

ードがパス検索を始めると、容易に通信不能となる。したがって、これらのアルゴリズムには、ネットワーク閉鎖を防ぐメカニズムがあるべきである。

3.3 VPC on KODAMA を用いたアクセス制御とルーティング

VPC on KODAMA をセンサネットワークに適用することによって、センサネットワークはアクセスとルーティングのコントロールの能力を持つことができる。また、アプリケーションに応じて、VPC on KODAMA は適切なモジュールをノードが動的に得るメカニズムに供給する。VPC on KODAMA を用いたセンサネットワークとノードの構造を図 3 に示す。

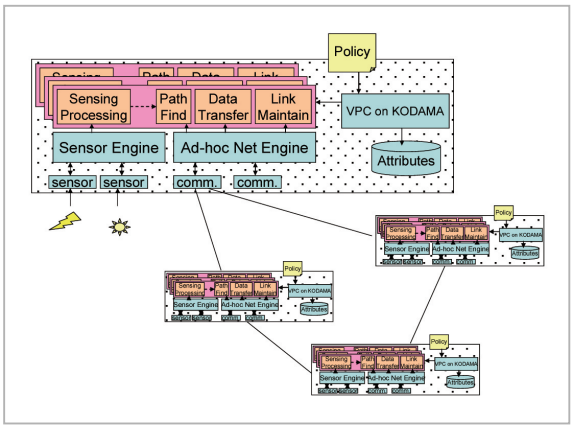

図3 VPC on KODAMA を用いたセンサネットワークのアーキテクチャ

各センサノードは、センサエンジン、アドホックネットワークエンジン及び VPC on KODAMA エンジンを持つ。VPC on KODAMA エンジンは、センサノードの属性を管理し、ポリシの受入れを行う。一つのポリシは、センサ処理モジュールや経路発見モジュールなどのアドホックネットワークモジュールを含む。

VPC on KODAMA エンジンは、ポリシを自身の属性を元に評価し、センサ情報処理モジュール、経路発見モジュール、データ転送モジュール及びリンク維持モジュールを決定する。

アドホックネットエンジンは VPC on KODAMA によって選択されたモジュールを実行する。アドホックネットエンジンは、経路検索モジュールの振舞いに従ってアドホックネットワークを形成し、データ転送モジュールによりデータを転送し、リンク維持モジュールによりリンクを維持する。

センサエンジンはセンサノードの持つセンサを管理する。センサエンジンがどうセンサを扱うかは、VPC on KODAMA エンジンによって決定されたモジュールの処理による。センサ情報処理モジュールは、ノードがセンサからデータをどのように得るか、ノードがどのようにデータを処理するか、さらに、ノードがデータをどこに転送するかを決定する。

このアーキテクチャは、各ノードが適切なセンサから必要なデータを得て、データを処理して、アプリケーションのポリシに応じてデータを適切なノードを転送することを可能にする。幾つかのノードの処理は異なる場合においても、このアーキテクチャでは適切な処理が適切なノードにインストールされる。また、このアーキテクチャは、ユーザが容易にアプリケーションをインストールするのを可能にする。TTL (Time To Live) が切れるまで、ポリシはノードの中で伝播される。ユーザは、どのノードにどのモジュールがあるべきであるかを考える必要はない。

4 アプリケーション

このセクションは、VPC on KODAMA を用いたアクセス管理とルーティングの応用例を RFID センサネットワークとして述べる。

このアプリケーションは、ある領域にいるユーザの位置を検出することを目的とする。このアプリケーションのセンサネットワークは自動的に検出される ID によって振舞いを変える。各ユーザはそれ自身の ID を定期的に送るアクティブ RFID タグを持つ。領域に対応するよう配置された RFID 受信機が ID を受信し、特定のサーバにその情報を通知し、サーバで ID を持つユーザの位置を計算するシステムである。ID によって、サーバは異なっている。ID が個人情報であるので、適切なサーバはデータを扱うべきである。

図 4 はシステムの概観を示す。このシステムでは、二つのサーバ、二つのタイプのセンサと

RFID タグの二つのタイプがある。一つのタイプのサーバ、センサ及びタグは VIP ユーザのためのものであり、他方は一般ユーザのためのものである。サーバはユーザの情報を管理する。VIP サーバは VIP ユーザの情報を管理する、そして、他方は残りのユーザを管理する。各センサノードは、VPC on KODAMA の枠組みを持ち、アクティブ RFID タグのセンサとアドホックネットのエンジンを持つ。VIP 用のセンサと他のものの唯一の違いは証明書である。VIP 用のセンサは、VIP サーバが発行した証明書を持ち認証されている。センサエンジンとアドホックネットのエンジンは、VIP 用と一般用で同じものである。タグは定期的にそれら自身の ID を送る。VIP タグの ID は暗号化されているが、一般向けのタグは暗号化されていない。

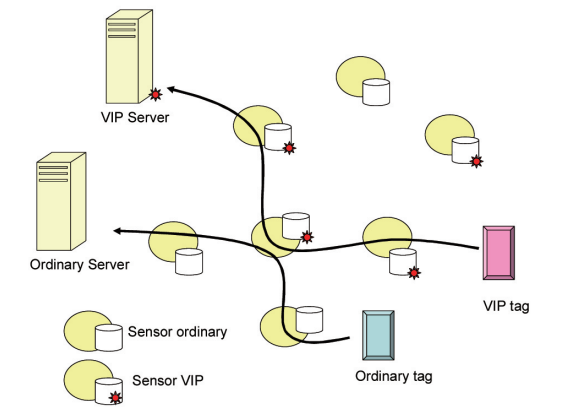

図4　システム概要

図 5 はこのシステムのポリシを示す。センサノードに VIP サーバの証明書があるなら、センサノードは役割の「VIP RFID sensor」を持つことができる。また、すべてのセンサが「normal RFID sensor」として作動することができる。ポリシは、XML によって書かれていて、署名がある S/MIME によって署名がなされる。各センサは、署名をチェックすることで、ポリシが本物であるかどうかを検知することができる。

役割の「VIP RFID sensor」は、VIP タグ検出モジュール、署名付き経路発見モジュール、信頼できるノードへのデータ転送モジュール（信頼転送モジュール）及びリンクチェックモジュールから成る。VIP タグ検出モジュールは、暗号化さ

```
<rule>
   <condition> eq VIP certificate </condition>
   <role> VIP RFID sensor </role>
</rule>
<rule>
   <condition> TRUE </condition>
   <role> normal RFID sensor </role>
</rule>
                              …
<role>
   <role name> VIP RFID sensor </role name>
   <module> VIP tag detection </module>
   <module> finding path with signature </module>
   <module> reliable forwarding </module>
   <module> polling link check </module>
</role>
                              …
<role>
   <role name> normal RFID sensor </role name>
   <module> RFID detection </module>
   <module> path finding </module>
   <module> sending </module>
   <module> polling link check </module>
</role>
                              …
```

図5　割付ルールと役割の定義

れている VIP タグのみ検出可能である。署名付き経路発見モジュールは、VIP サーバまでの経路を発見する。このモジュールは以下のアルゴリズムを持つ。(1) モジュールはノードの署名をつけて目標ノードへの要求メッセージをブロードキャストする。(2) 目標ノードでないノードはメッセージに自身の ID を署名し、メッセージを隣接モジュールへ転送する。(3) 目標ノード（VIP サーバノード）は要求メッセージが持つ署名リストをチェックする。もし、すべての署名が本物である場合、要求メッセージを発信したノードへ、署名リストとは逆の経路で、署名リストとともに応答メッセージを返す。その経路上にあるノードは、署名リストから VIP サーバと発信元ノードに対応する隣接ノードを経路として記憶する。VIP サーバノードは、自身が発行した証明書を持たないノードがリスト上にある場合は破棄する。したがって、VIP センサノードは、VIP RFID sensor だけで構成された安全な経路を作成することができる。信頼転送モジュールは、ノードの署名と共に検出された暗号化されたタグ ID をそのまま VIP サーバに対応する隣接ノードに送る。このとき、送信した隣接ノードからの ack を受ける。VIP サーバだけが暗号化された ID を解読することができる。これにより安全かつ確実にデータをサーバに送ることができ

る。リンクチェックモジュールは定期的に「Hello」メッセージを隣接に送り、隣接ノードが有効化どうかを確認する。

また、役割の「normal RFID sensor」は、RFID検出モジュール、経路発見モジュール、転送モジュール及びリンクチェックモジュールから成る。RFID検出モジュールは、一般のRFIDタグを検出することができて、VIP RFIDタグは検出することができない。経路発見モジュールはノードの署名なしで要求のブロードキャストで経路を見つける。送付モジュールはackなしで検出されたIDを一般サーバに送るだけである。

ユーザはこのポリシをセンサネットワークの一つのノードに渡す。センサノードはそのポリシを互いにコピーする。VIPセンサ(証明書を持っている)に方針があるとき、それらは「VIP RFID sensor」と「normal RFID sensor」として機能する。それらは、VIPセンサノードを通して安全にVIPサーバにVIPタグを検出したデータを転送する。VIPセンサは、また、一般タグを検出して、データを一般サーバに転送することができる。他のセンサ(証明書を持っていない)は「normal RFID sensor」として作動する。それらは一般のRFIDタグを検出して、データを一般サーバに送る。

このように、ポリシに応じて、センサは役目を変える。ユーザはポリシをすべてのセンサノードに渡す必要はない。また、適切なモジュールは適切なノードにインストールされる。

5 関連研究

MOTE[1]はセンサネットワークモジュールである。MOAP[2]はセンサノードにプログラムコードを分配するプロトコルである。INSENSE[9]は無線のセンサネットワークにおいて、侵入耐性があるルーティングプロトコルである。SIA[10]には、質問で手当たりしだいに不法なノードを検出するメカニズムがある。

MOTEはハードウェアとソフトウェアプラットホームをセンサネットワークに提供する。MOTEのソフトウェアプラットホームはダイナミックにプログラムコードを受け入れることができる。しかしながら、ユーザは、直接コードを各ノードに送る必要がある。センサネットワークのためのVPC on KODAMAは直接プログラムコードをユーザが送る必要はないメカニズムに与える。

MOAPはマルチホップネットワーク・プログラミングの実装である。マルチホップネットワーク・プログラミングの挑戦の一つはネットワークを飽和状態にしないでプログラムコードを複数のセンサノードに伝播することである。MOAPはネットワークをあふれさせないで、プログラムコードパケットを選択している数のノードに広めるために、Ripple disseminationプロトコルと呼ばれるアルゴリズムを使用する。MOAPの目的はすべてのノードに同じプログラムコードを分配することである。したがって、ノードに依存するプログラムコードを変えるのは難しい。センサネットワークのためのVPC on KODAMAは、ノードに依存するプログラムコードを分配するためにメカニズムを提供する。

INSENSEのセンサノードは、幾つかの経路でノードを対象とするために検知データを送る。目標ノードが幾つかの経路を通り抜けるデータをチェックするとき、センサネットワークは不法なノードを検出することができる。ノードが複数回同じデータを送るので、INSENSEの通信コストは高い。VPC on KODAMAのノードの保護メカニズムは複数回同じデータを送らないで安全な通信を提供する。VPC on KODAMAのセンサノードは署名で不法なポリシをチェックすることができる。処理が耐タンパデバイスで照合処理は行われる。このように、このメカニズムは物理的、そして、プログラム攻撃を防ぐことができる。

SIAは質問で不法なノードをノードが検出するメカニズムに定期的に供給する。このメカニズムはネットワーク資源を消費する。SIAのモデルは主要なサーバのコントロールである。センサネットワークには一つのサーバがある場合では、このモデルはうまく動作する。しかしながら、サーバが複数あるか、又は各ノードが互いに通信するなら、質問のための通信コストは高価過ぎる。センサネットワークのためのVPC on KODAMAは署名を信用できるノードのための枠組みに提供する。

6 まとめ

この論文はポリシ規制センサネットワークの新しい枠組みについて述べた。VPC on KOMADA に基づいているこの枠組みは、センサノードが適切なモジュールをポリシにより持つことを可能とする。ユーザが安全にアプリケーションポリシをセンサネットワークに投入するだけで、センサノードはアプリケーションにおける適切な役割を実行する。なお、VPC on KODAMA は、平成 13 年から 15 年の間、旧 TAO の研究委託「相互接続時のセキュリティポリシ管理技術に関する研究開発」の成果である。

センサノードでは、ネットワーク、アプリケーションの多様性とセキュリティは重要である。アプリケーションの多様性を増加させるように、センサノードは、ダイナミックにアプリケーションモジュールを受け入れて、また、適切なモジュールを持つ必要がある。センサノードがどのようにデータを検出して、データを処理して、データを送るかはアプリケーションによる。適切な検出モジュールとネットワークモジュールはインストールされるべきである。また、センサネットワークは、不法なアクセスに対して保護されるべきである。同時に、それらの検知データは保護されるべきである。

センサネットワークのための VPC on KODAMA は、センサノードが、アプリケーションのポリシとそれぞれのノードの属性に従って適切な検出モジュールとネットワークモジュールを決定することを可能とする。各ポリシには署名がつけられており、各ノードはその署名を確認することで本物かどうかを検出することができる。また、安全な装置で役割の決定を行うため、不法な装置は役割を得ることができない。

例として検出された RFIDs に対応する振舞いを変えるセンサネットワークを示した。それらの属性と方針により、センサノードはそれら自身の役割を変え、安全なセンサネットワークをとして機能する。VIP タグを扱うことができるノードだけが、安全にタグを検出して、認可されたノードを通してデータを転送する。VIP サーバだけが VIP タグの ID を知ることができる。

このように、センサネットワークのための VPC on KODAMA は、センサネットワークに適した枠組みである。今後、軽量実装についての議論をし、実際の装置で枠組みを開発する予定である。

参考文献

1 J. Jong and D. Culler, "Incremental Network Programming for Wireless Sensors", IEEE SECON 2004.
2 Thanos Stathopoulos, John Heidemann, and Deborah Estrin, "A Remote Code Update Mechanism for Wireless Sensor Networks," CENS Technical Report #30, http,//lecs.cs.ucla.edu/thanos/moap-TR.pdf
3 T.Iwao, S.Amamiya, K.Takahashi, G.Zhong, T.Kainuma, L.Ji, and M.Amamiya, "An Information Notification Model with VPC on KODAMA in an Ubiquitous Computing Environment, and Its Experiment", CIA 2003, pp.30-45, 2003.
4 K.Takahashi, S.Amamiya, T.Iwao, G.Zhong, and M.Amamiya, "Testing of Multi-agent-based System in Ubiquitous Computing Environment", KES 2004, pp.124-130, 2004.
5 T.Iwao, S.Amamiya, G.Zhong, and M.Amamiya, "Ubiquitous Computing with Service Adaptation Using Peer-to-Peer Communication Framework", FTDCS 2003, pp.240-248, 2003.
6 G.Zhong, S.Amamiya, K.Takahashi, T.Iwao, K.Kawashima, T.Ishiguro, T.Kainuma, and M.Amamiya, "You've Got Mail From Your Agent : A Location and Context Sensitive Agent System", ESAW 2003, pp.392-409.

7 A.Bruce McDonald and Taieb Znati "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks", IEEE Journal on Selected Areas in Communication, Vol.17, No.8, Aug. 1999.

8 Sung-Ju Lee,William Su and Mario Gerla,"Ad hoc Wireless Multicast with Mobility Prediction", To appear in Proceedings of IEEE ICCCN'99, Boston, MA, Oct. 1999.

9 Deng, J., Han, R., and Mishra, S., "A performance evaluation of intrusion-tolerant routing in wireless sensor networks", In proceedings of the 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN 2003), pp.249-364, 2003.

10 Przdatek, B., Song, D., and Perrig, A., "SIA, Secure information aggregation in sensor networks", In proceedings of the 1st ACM International Conference on Embedded Networkd Sensor Systems, ACM Press, pp.255-265, 2003.

岩尾忠重（いわおただしげ）
富士通株式会社ユビキタス事業本部ユビキタス推進統括部ユビキタスビジネス推進部　博士（工学）
マルチエージェントシステム、センサーネットワーク、アドホックネットワーク

雨宮真人（あまみやまこと）
九州大学大学院システム情報科学研究院知能システム学部門教授　工学博士
超並列分散処理アーキテクチャ、並列分散知能処理システム、マルチエージェントシステムなど