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内では、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備付け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、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ー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ー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、そのポリシーをもとに、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、ポリシー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。

近い将来セカン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、セカン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カン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一緒にセカンネットワーク上で動作することになる。そのような状況においては、セカンネットワークは、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単純であるべきである。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、セカンネットワークでは、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。セカン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。セカンネットワークが単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、セカンネットワークには、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ツールが必要である。

我々は、セカンネットワークの新しいツールを提案する。このツールは、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 とする。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、互いに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識して、安全に役割を割り当てるための機能を持つ。セカンネットワークでは、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 をセカンネットワークに適用することによって、セカンネットワークは、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カンネットワークのコントロールについて述べる。セカン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 となりポリシによりセカン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 多目的セカンネットワークにおけるポリシ

2.1 多目的セカンネットワークの要件

セカンネットワークでは、多くのセンサーを物理現象を検出し、その検出データを処理して、互いに通信する特徴がある。多目的のセカンネットワークでは、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。多目的のセカン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の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、各センサノードは動的にアプリケーションの受け入れを可能とするべきである。また、セカンネットワークのノード数は拡大す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、保護の仕方を変化するかもしれない。アプリケーションごとに必要なセキュリティの制御機関を取り入れることができるように機能を多目的センサネットワークの枠組みに持つべきである。このような、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て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。数多くのノードの役割が共存し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。このようなセンサネットワークにおけるノードの役割は同じではない。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の問題となる。二つ目の問題はインスタンスのジェネレーションが他のジョブと異なることである。両方の問題を解決するために、数多くのセンサノードでの各ノードには適切なジョブ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ンサネットワークに基づく重要な二つの点がある。一つは、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の不法なデータとアクセスを守るかということでもある。センサネットワークの保護は、データを検出し、処理し、そして転送することである。それぞれのプロセスにおいて、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し、転送するシーンである。センサノードが、検出されたデータを、物であるかどうか検出することができる、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、一般に、温度や湿度などの物理的な現象を、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、この場合にも、ダイナミックにモジュールを持つ能力は有効である。

次に、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。つまり、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、不正時のみ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。

最後に、ノードが処理データを他のノードに送る場面である。この場合における、データを送るような、もしも受け取るようなノードが信用できるかどうか試みなければならない。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与をするノードだけだが、データを互いに送るか、又は受け取ることができる場面である。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は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多くない。したがって、アプリケーションへの対応するノードは、特に自主的に論理的なネットワークを構築する必要がある。

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己的で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である。センサネットワークはセンサネットワーク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記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[10]-[16]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。別の条件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権格される。そのため、ユーザさえ属性を不正に変更することできない。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、ポリシ設定

![図1 パブリックポリシの構造](image-url)
リシの筆名をチェックして、条件を指すタンパク
バイスにある決断モジュールに送って、コミュニ
ティ内のそれを自身の役割を得る。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[2][8]は、動的にノー
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、目標ノードに送るのに適切な接続ノー
ドを選択し、受信データの転送を繰り返す。こ
の結果、一つ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
ードがどの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接続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。接続ノード
が通信しきれないなら、ノードは、別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接続ノードを知ることができる。ノードは、接続ノードが利用可能である
間、データを接続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
ードは、接続ノードの移動や機能不全が起こるこ
とも考慮し、接続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。接続ノードが利
用不可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
ードは同じルートを繰り返す。

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選択するべきである。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、信頼性よりも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、データ転送方法
も物理現象のデータと人間的なデータで異な
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である。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、内部から
適切なアルゴリズムを選択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。視覚的
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
ードがうまく動作しているように思えても、ネッ
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
容量を超えると、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

図2 アドホックネットワークの機能の関係

NICT 201
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 をセカンテネットワークに適用することによって、セカンテネットワークはアクセス制御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 を用いたセカンテネットワークとノードの構造を図 3 に示す。

![図3 VPC on KODAMA を用いたセカンテネットワークのアーキテクチャ](image)

各セカンノードは、セカンエンジン、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、セカンのノードの性質を管理し、ボリシの受け入れを行う。一つのボリシは、セカン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、ボリシを自身の性質を元に評価し、セカン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。

セカンエンジンはセカンノードの持つセカンを管理する。セカンエンジンがどうセカンを扱うのかは、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。セカン情報処理モジュールは、ノードがセカン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のよう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カン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関じてデータを適切なノードに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、ボ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 セカン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カンネットワークは自動的に検出される ID を通じて振舞いを変える。各ユーザはそれぞれ自身の 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に配置された 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ー、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。サーバーはユーザの情報を管理する。VIP サーバーは 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。各センサーは実装した KODAMA の構組みを持ち、アクティブ RFID タグのセンサとアドレスネットワークのエンジンを持つ。VIP 用のセンサと他のも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制御されている。センサは、RFID エンジンとアドレスネットワークのエンジンは、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5 割り配ルールと役割の定義

図5 はこのシステムのポリシーを示す。センサーノードに VIP サーバーの証明書があるなら、センサーノードは役割の「RFID sensor」を持つことができる。また、すべてのセンサが「RFID sensor」として作動することができる。ポリシーは、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、ポリシーが本物であるかどうかを検証することができる。

役割の「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プロードキャストする。2) 目標ノードで署名の署名はメッセージに自身の ID を署名し、メッセージを接続モジュールへ転送する。3) 目標ノード（VIP サーバー）は署名メッセージの署名の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。その経路上であるノードは、署名リストから VIP サーバと発信元ノードに対応する接続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を破棄する。したがって、VIP センサーノードは、VIP RFID sensor だけでなく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 サーバに対応する接続ノードに送る。このとき、送信した接続ノードからの ack を受ける。VIP サーバだけが暗号化された ID を解釈することができる。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
ル。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かどうかを確認する。
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プローフォーマーで経路を見つける。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ーをセンサネットワークの一つのノードに渡す。センサネットワークはそのポリシーや記入する。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センサネットワークを通じて全てのVIPサーバにRFIDタグを検出され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、ポリシーより、センサは役目を変える。ユーザはポリシーよりすべてのセンサネットワークに渡す必要はない。また、適切なモジュールを適切なノードにインストールされる。

5 関連研究

MOTEはセンサネットワークの一つのモジュールである。MOAPはセンサネットワークプログラムコードを分配するプロトコルである。INSENSE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は、質問と答えの一部で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らせずで、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のセンサネットワークは、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じ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ーをチェックすることができる。処理が耐タンパクサイズ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のモデルは一つの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作動する。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、質問の中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作成、センサネットワークに投入できる。なお、VPC on KOMADA 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ために、センサノードは、ユーザがアプリケーションモジュールを受け入れ、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、他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 KOMADA 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ており、各ノードはその署名を確認することで不法な操作を行うことができ、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。それらの属性と方向により、センサノードはそれら自身の役割を変える、安全なセンサネットワークとして機能する。VIP ツ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じてデータを転送する。VIP サーバだけが VIP ツグの 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 KOMADA は、センサネットワークに適した枠組みである。今後、検知実装についての議論を、実際の装置で枠組みを開発する予定である。

参考文献

