様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 6 月 20 日現在

研究種目：若手研究(B)
研究期間：H20～H21
課題番号：20700055
研究課題名（和文）　セキュアなセンサネットワークを実現するセンサノードの相互監視システムの設計
研究課題名（英文）　Research on the design of monitoring system of sensor nodes for secure sensor networks

研究代表者
角田　裕（Hiroshi TSUNODA）
東北工業大学・工学部・講師
研究者番号：30400302

研究成果の概要（和文）：様々な物理情報の観測と収集への利用が期待されるセンサネットワークは,従来のネットワーク以上に実世界･物理世界に密着した情報を運ぶネットワークであり、そのセキュリティの確保は，センサネットワークの安全な利活用に必須である。本研究では、キュアなセンサネットワークの構築に必要な、センサ間の監視方式、ネットワーク内の不正アクセスの追跡方法、管理ログの収集方式を検討し提案した。

研究成果の概要（英文）：A sensor network is a promising technology for collecting various physical data, and carry data are closely-attached to our real life. Therefore, security is a fundamental requirement in sensor networks. In this study, for constructing secure sensor networks, monitoring system for detecting suspicious sensor nodes, DoS traceback method, and log collection system are proposed.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
平成 20 年度	1,400,000	420,000	1,820,000
平成 21 年度	900,000	270,000	1,170,000
総　計	2,300,000	690,000	2,990,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：センサネットワーク，セキュアネットワーク

１．研究開始当初の背景

近年の無線通信および小型デバイス技術の進展によって､超小型の ID タグ(RFID)や、様々なセンサを備えた小型センサノードからの無線通信を介した情報の取得が可能となり、これらからの情報収集技術が我々の生活の安全・安心面を支える重要な基盤となりつつある。例えば、RFID は食品や医薬品に添付されることで、それらの商品のトレーサビリティを保証する要となる。また、小型で安価なセンサノードの利用により、火山活動や地震の観測など広域環境の観測から、家屋への不法侵入の検知など個人レベルでの監視まで、様々な観測・監視の網を柔軟に展開することが可能となる。この柔軟な観測・監視網の展開は、センサノード同士が相互接続し、センサノード間でパケットを繰り返し中継するアドホック通信によって、観測データをデータ収集ノードにまで送信することで可能となる。

その用途からわかる通り、無線センサネットワークはインターネット以上に実世界・物

理世界に密着した情報を運ぶネットワークである。すなわち、ネットワーク上を流れる情報の改ざんや欠損の発生が、不法侵入の見逃しなど実世界に対する実質的な悪影響を及ぼす危険性がある。それにも関わらず、インターネットの研究開発の過程でデータの効率的な送受信を実現することのみが重視され運用面やセキュリティ面が後手に回ってしまったのと同様に、無線センサネットワークにおいてもネットワーク技術の研究開発のみが先行し、その結果運用管理やセキュリティ管理に関する検討が立ち遅れている。そのため、センサノードが悪意ある攻撃者の手によって不正に操作され、中継すべきデータが意図的に改ざん・破棄をしたり、不要なデータを大量に送出するような異常な動作を始めた場合に、それを検知するための方式が確立されていない現状にある。現在期待されているような多くの分野での無線センサネットワークの利活用の実現には、安全なネットワークを通じて情報が収集され、利用者に安心して情報を活用できることが必須である。すなわち、「安全性の確保」というハードルをクリアすることが、無線センサネットワークが利用者にとって信頼できる有用な情報収集インフラとなるための喫緊の課題である。

２．研究の目的

背景で述べたように、無線センサネットワークにおいてデータを中継するノードが攻撃者によって乗っ取られたり、不正な動作をするよう設定されたノードに置き換えられたりした場合、データの収集に致命的な障害を被る。本研究は、このようなアドホック通信を行う無線センサネットワークの有用性と対をなすセキュリティ面での脆弱性の克服を目指す。セキュアな無線センサネットワークの実現には、各センサノードの動作の監視が必要であるが、無数のセンサノードで構成されその構成が時間と共に変化しうるアドホックセンサネットワークにおいては集中型の監視システムは適さない。本研究では、すべてのセンサノードが監視機能を有する相互監視型のシステムを前提としたシステムについて検討する。

３．研究の方法

本研究では、まず必要最小限のノードによる監視を実現するために、少数の監視ノードから監視を始め、次第に他のノードに監視の開始を指示する協調型監視方式について検討した。また、並行してセンサネットワークにおいて問題となる具体的な不正アクセスとしてサービス拒否攻撃への対抗策および監視システムの運用を効率化するログ転送方式について検討した。

４．研究成果

図１は、本研究で提案する協調型監視の概要を示している。協調型監視では、継続的に周囲のノードを監視する「監視ノード」と必要に応じて監視ノードから駆動される「サブ監視ノード」に分かれる。監視ノードとサブ監視ノードの動作のフローチャートを図２に示す。

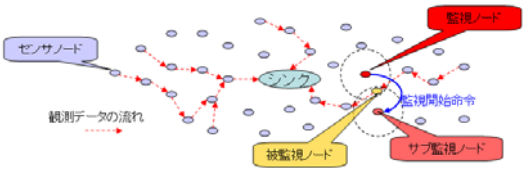

図 1 協調型監視の概要

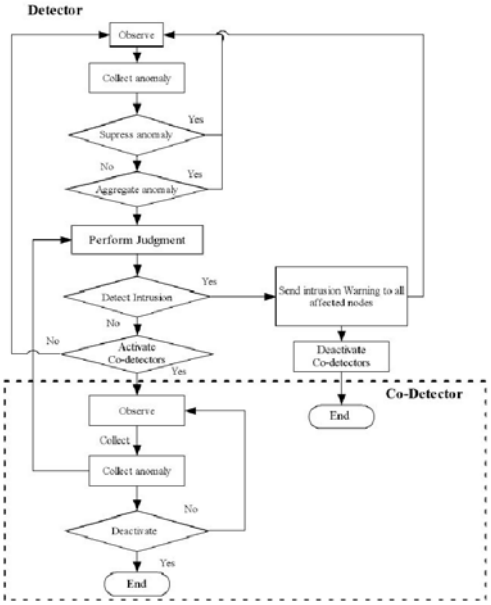

図 2 監視ノードとサブ監視ノードの動作

監視ノードは、被監視ノードのパケット中継動作を監視し、中継すべきパケットを破棄するなどの不審な挙動が見られる場合に、それをより多方面から分析するために、周囲のノードの監視機能を駆動し、サブ監視ノードとする。サブ監視ノードは、同様に周囲のノードの挙動を監視し、不審な挙動を発見した場合には自身を駆動した監視ノードに通知する。監視ノードは、自身の監視結果とサブ監視ノードから集まった情報に基づいて被監視ノードが侵入された異常ノードかどうかを判断し、異常が認められた場合にはシンクに対してアラートを送信すると同時に、周囲のノードにワーニング送信する。このワーニングはすでに検知済みのノードに対して複数の監視ノードが同内容のアラートを送信することを防止するために使用される。こ

れにより、バッテリー駆動のセンサノードで構成され省電力化が強く要求される無線センサネットワークにおいて、効率的な検知動作が実現できる。ソフトウェアによるネットワークシミュレーションを通じ、提案手法が優れていることを確認した。

次に、本研究ではセンサネットワークのような移動体ネットワークにおけるサービス拒否(DoS: Denial of Service)攻撃の脅威に着目し、その追跡方式について検討した。既存の DoS 攻撃追跡手法は有線ネットワークにおける適用を想定しているため移動体ネットワークには適さないものが多く、移動体ネットワークに適した手法であっても非実用的という問題点がある。さらに、移動体ネットワークは移動端末の無線リンク部分が狭帯域であると共に、端末は自由にネットワーク間を移動する。そのため、帯域の有効利用が重要であり、そのため追跡メカニズムの導入によって帯域を圧迫しないことが移動体ネットワークにおける DoS 攻撃追跡手法には重要であった。攻撃者が移動可能であることから、追跡により攻撃元のネットワークを特定できたにも関わらず、攻撃者が既に別のネットワークへ移動済みであることを防ぐために、短時間で追跡完了することが重要な要件であった。そこで、帯域を圧迫しないこと、および短時間で追跡を完了することを満足するような DoS 攻撃追跡手法として、既存の DoS 攻撃追跡手法である iTrace とその派生技術を発展させた手法を提案した。提案方式は、通常は等確率で生成される iTrace メッセージを攻撃者からのホップ数に基づいた確率により生成するもので、移動体ネットワークにおいても効果的に DoS 攻撃を追跡することができる。提案手法の有効性は、移動体ネットワークを模擬したネットワークシミュレーションにより示した。

相互監視システムでは、各ノードからの監視結果をログとして収集する必要がある。このとき必要とされるのは、ログ全体の収集の信頼性と重要なログに関する収集のリアルタイム性である。そこで、本研究では、センサネットワークにおいて無線リンクを経由してログが収集されることを考慮し、ログの重要度に基づく集約と優先キューイングを行う、効率的なログ転送方式を提案した。インターネットを例にとると、ログの収集には UDP によるトランスポートを基本とした Syslog プロトコルが広く用いられ、収集の信頼性を確保するために TCP の利用が広がっている。しかし、TCP は通信制御にログの重要度を考慮しないため、重要なログの送信が遅延する問題があり、無線リンクにおける通信の断絶がこの問題を助長する。そこで、本研究では、UDP とアプリケーションレベルでの確認応答を組み合わせ、図 3 に示すように各アプリケーションからのログを、その重要度に基づいて優先キューイングを行い、さらにログの集約を行う、重要なログの転送時間と送信データ量の双方を削減する方式を提案した。実験ネットワークを用いた評価の結果、優先キューイングにより切断されていた無線リンクの回復後に効率的に重要度の高いログを送信できることを示した。またキュー内にログが蓄積されている時間を活用し、ログの内容に基づいて集約を行うことで、転送するログのサイズを削減できることを示した。

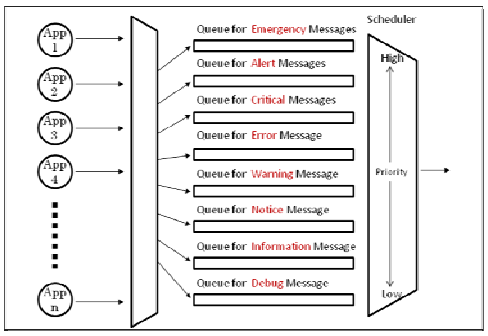

図 3 ログの重要度に基づく優先キューイング

５．主な発表論文等

〔雑誌論文〕（計 5 件）

1. “Wireless Telemedicine Services Over Integrated IEEE 802.11/WLAN and IEEE 802.16/WiMAX Networks”, Yan ZHANG, Nirwan ANSARI, and Hiroshi TSUNODA, IEEE Wireless Communications Magazine Special Issue on “Wireless Technologies for E-healthcare”, Vol. 17, Issue 1, pp.30-36 Feb.2010 (査読有)

2. “地理的位置情報と軌道情報を併用した Walker Delta型LEO衛星ネットワーク向け移動管理方式”角田 裕, 太田 耕平, 根元義章, 電子情報通信学会論文誌B, Vol.J91-B, No.12 ,pp.1600-1610, Dec. 2008 (査読有)

3. “Detecting DRDoS Attacks by a Simple Response Packet Confirmation Mechanism”, Hiroshi TSUNODA, Kohei OHTA, Atsunori YAMAMOTO, Nirwan ANSARI, Yuji WAIZUMI, and Yoshiaki NEMOTO, Comupter Communications, Vol.31, 2008, pp.3299-330, Sep. 2008 (査読有)

4. “Improving the Efficiency of DoS Traceback Based on the Enhanced ITrace-CP Method for Mobile Environment”, Hiroshi TSUNODA, Taishi TOCHIORI, Yuji WAIZUMI, Nei KATO, and Yoshiaki NEMOTO, Proc. of International Conference on Communications and Networking in China (CHINACOM), 2008, pp.680-685, Aug. 2008 (査読有)

5. “Detecting Pulsing Denial-of-Service Attacks Based on the Bandwidth Usage Condition”, Hiroshi TSUNODA, Kenjirou ARAI, Yuji WAIZUMI, Nirwan ANSARI, and Yoshiaki NEMOTO, Proc. of IEEE International Conference on Communications, 2008, pp.1670-1674, May 2008 (査読有)

〔学会発表〕（計 2 件）

1. “ログの重要度に基づく優先キューイングと集約による無線リンクを考慮したログ転送の効率化”, 角田裕，真下浩平，和泉勇治, 根元義章， 電子情報通信学会通信方式研究会，2009 年 9 月 10 日，東北大学電気通信研究所

2. “パルス型DoS攻撃の影響と検知システムに関する検討, 熊坂祥貴，北川康彦，角田裕，東北地区若手研究者研究発表会，2009 年 2 月 26 日，東北学院大学工学部

3. “Improving the Efficiency of DoS Traceback Based on the Enhanced ITrace-CP Method for Mobile Environment”, Hiroshi TSUNODA, Taishi TOCHIORI, Yuji WAIZUMI, Nei KATO, and Yoshiaki NEMOTO, International Conference on Communications and Networking in China (CHINACOM) 2008, Aug.26th 2008, Hangzhou, China

4. “Detecting Pulsing Denial-of-Service Attacks Based on the Bandwidth Usage Condition”, Hiroshi TSUNODA, Kenjirou ARAI, Yuji WAIZUMI, Nirwan ANSARI, and Yoshiaki NEMOTO, IEEE International Conference on Communications, 2008, pp.1670-1674, May 22th 2008, Beijing, China

６．研究組織

(1)研究代表者

角田　裕（Hiroshi TSUNODA）
東北工業大学・工学部・講師
研究者番号：30400302