科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２１　日現在

機関番号：　１４６０３
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７０００８４

研究課題名（和文）安全・安心なＩＴＳアプリケーションのためのセキュリティ機構に関する研究

研究課題名（英文）Proposal of a secure mechanism for ITS application and its implementation.

研究代表者
猪俣　敦夫（INOMATA, ATSUO）

奈良先端科学技術大学院大学・総合情報基盤センター・准教授

研究者番号：９０５０５８６９

交付決定額（研究期間全体）：（直接経費）　　2,200,000円、（間接経費）　　660,000円

研究成果の概要（和文）：本研究では、高度道路交通システム（ITS）アプリケーションに対するセキュリティ機構を提案する。大半を担うノードは車であることから、その移動によりネットワーク構成が変動するため、必要なサービスを短時間のうちに、低コストかつ正確に保証された情報として発見することが難しい。現状、プライバシの観点からのセキュリティ機能も有していないため、セキュアなサービスディスカバリ機構の実現は急務である。フランス国立情報学自動制御研究所と進めてきたITSアーキテクチャ上で動作するITS向けセキュリティ機構として、より効率の良いセキュリティプロトコルを楕円曲線暗号ベースのモデルを設計し、実機を用いた評価を行う。

研究成果の概要（英文）：In this research, I propose a security mechanism for ITS(Intelligent Transportation System) application.
From the node responsible for the majority is CAR in ITS, because the network configuration may drastically change depending on the movement, to discover required service as guranteed accurate and low cost within a short period of time is difficult. Now ITS does not have any security features in terms of privacy, to establish more secure service discovery mechanism is urgent issue.
As a security mechanism runs on ITS architecture that has been working with INRIA(Institut National de Recherche en Informatique et Automatique), I design a more efficient model of an elliptic curve cryptography based security protocols and execute an evaluation on the real actual equipment.

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：　セキュリティ　プライバシー　ITS　位置情報

１．研究開始当初の背景

ITS（Intelligent Transportation System : ITS）は、車両、道路、路側の建造物、および交通利用者をネットワーク接続することにより、交通安全の向上、交通管理の最適化（渋滞解消、緊急車両の経路確保等）、利用者（運転者、同乗者、および歩行者）への付加価値提供を行う。近年、国際標準化機構(ISO)、欧州電気通信標準化機構(ETSI)、および各国の研究機関が産・学連携して ITS 通信基盤（ITS コミュニケーションアーキテクチャ）の標準化を推進している。このアーキテクチャは ISO/OSI モデルを基盤としつつ、次の 4 つの先進的機構：

(1)複数の通信デバイスの同時制御
(2) 車々間アドホックネットワーク (Vehicular Ad-Hoc Networking; VANET)
(3)ネットワークモビリティをサポートするプロトコル(Network Mobility basic support protocol; NEMO)を用いた車両の移動に依存しない永続的なインターネット接続の提供
(4)地理位置を基準とした通信機構

を備えている。こうした背景の下、ITS におけるアプリケーションは、上述したアーキテクチャ共用の「サービス」と呼ばれる基本機能の連携によって実現される（例えば、駐車場制御アプリケーションは「接近車両の検知」、「電子ゲートの制御」、「支払い」の 3 サービスの連携によって実現できる）。これらのサービスは独立した 1 個の「手続き」に該当し、その用途に応じて乗り物、道路、ITS センター、およびインターネット上のサーバなど様々な計算機上に配置される。例えば、自動車や道路サービスとしては近隣エリアの事故検知サービスが配置され、ITS センターでは地図データの提供サービスが配置される、等である。

さらに、ITS アプリケーションでは各所に散在するサービスを、ピアツーピア接続を用いて連結することで、利用者に特定の利便性を提供することも可能である。しかし、ITS アプリケーションが所定の機能を実現するためには、各所に散在するサービスのうち必要なものだけを発見・選別する機能（サービスディスカバリ）が必須となる。例えば「交通状況の検出サービス」のうち、自車の走行予定経路上に存在するものだけを利用する、等があげられる。しかし、ITS の大半を担うノードは自動車であることから、その移動によってネットワーク構成が頻繁に変動してしまい、必要なサービスを短時間時間のうちに低コストであり、正確かつ保証された情報として発見することが難しい。さらに、既存のサービスディスカバリプロトコルは上述した先進的機構を扱うべく設計されていないだけでなく、ノード、ユーザごとの情報を隠蔽する等プライバシの観点からのセキュリティ機能も有していない。このため、ネットワーク構成の変化に対応できる安全・安心なサービスディスカバリ機構の実現は急務である。

２．研究の目的

本研究では、高度道路交通システム（ITS）アプリケーションに対するセキュリティ機能・性能要件の洗い出しを行い、より安全性の高い、かつ効率の良い新しい ITS 向けセキュリティプロトコルの実現を目指す。ITS では各所に散在するサービスのうち必要なものだけを発見するサービスディスカバリが重要である。既に INRIA と検討を進めてきた ITS アプリケーションを実現するクロスレイヤモデル上のセキュリティ機能を確立するために、ペアリング暗号ベースのプロトコルを設計し、Android 端末上にプロトタイプを実装し、さらにその有用性評価のために現実環境 ITS テストベッドに適用し、評価を行い、社会実装の可能性

を探ることが本研究の狙いである。

３．研究の方法

ITS アプリケーションにおけるセキュリティ要件の基礎調査から開始を行う。これは、ITS のための基本プラットフォームとそのセキュリティ機能の関係を明確にする必要があることが理由である。具体的には、セキュリティの観点から SOA を用いたユーザ要求の洗い出しを行い、セキュリティ機能の定義を行う。

続いて、セキュリティを考慮した VANET と NEMO の協調の検討を行い、ITS アプリケーションのためのレイヤ横断型システム管理機構（クロスレイヤ）上でペアリング暗号ベースの効率の良いセキュリティプロトコルを設計し、Android 端末上にプロトタイプ実装を行う。

実装したプロトタイプを実機にインストールを行い、実記を用いた実験と評価としてセキュリティプロトコルの安全性とパフォーマンスを評価するために、大学が保有する ITS に必要な諸機能（GPS、モバイルルータ、各種センサ等）を装備した自家用自動車と、プロトタイプが実装された Android 端末とを連結し、評価を行うこととする。

４．研究成果

平成 23 年度

ITS アプリケーションの安全性に関する要求要件の洗い出しとして、適切な通信デバイス（例えば 802.11a/b/g/p, 2G or 3G 等）選択において、必要な機能の選択を実施した。本研究で特徴的なのは、実世界に存在する車を対象としているため、それぞれ車の位置情報をはじめとするプライバシを考慮したノード探索手法（安全なサービスディスカバリー機構と呼ぶ）を確立することにある。このサービスディスカバリ機構は、ISO/OSI モデルにおけるアプリケーション層に配置され、その下層の機能には関与しない。このため、サービスの探索対象は事前に割り当てられた特定の IP アドレスに固定され、サービスの発見の際にはアプリケーションの特性しか考慮しない（サービス名や事業者名等）ため、これが問題となる。そこで、対象とする ITS においては、複数の通信デバイスを通信状況に応じて使い分け、かつ不要な通信トラフィックの発生を避ける必要があり、クライアントのセキュリティ担保の観点からも、不特定デバイスとの通信や制御においてその安全性を保障する必要がある。さらに、状況によっては大量のメッセージ通信が行われるため、通信デバイスの性能・状況、あて先への経路、アプリケーションの通信頻度など複数のレイヤに属する情報を判断できるトレースバック機構も必要となる。

そこで、サーベイの結果得られたこれらの機能要件に対して設計したプロトタイプをシミュレーションベースで評価を行い、さらに一部実機（初年度においてはスマートフォンに実装はせず、ラップトップ PC）に実装し、実証実験を行った。この結果、通信デバイスの動的な選択および探索範囲の動的な調整においてセキュリティを保証する必要のある情報については整理することができた。これらの結果を踏まえ、効率の良い通信手段と認証方法を選択する必要があることが判明した。

平成 24 年度

初年度に得られた結果を踏まえて、ITS を対象としたノード間通信における効率よいサービスディスカバリ機構における、より安全な通信手段を提供するセキュリティプロトコルの開発を目指した。ITS においては、その大半を担うノードは自動車であるため、その移動によってネットワーク構成が頻繁に変動し、必要なサービスを短時間

のうちに、低コストで、かつ正確に保証された情報として見つけ出すことは難しい、それだけでなく、ノード・ユーザごとの情報を隠蔽する等プライバシの観点からのセキュリティ機能も有していない。これらの理由から、ネットワーク構成の変換に対応できる安全・安心なサービスディスカバリ機構の実現が急務であることを示した。そこで、研究提案者らがフランス国立情報学自動制御研究所（Institut National de Recherche en Informatique et Automatique : INRIA）と検討を進めてきたITSコミュニケーションアーキテクチャ上で動作するITSアプリケーションのための通信メカニズムにおけるセキュリティ機構として、より効率の良いセキュリティプロトコルの設計を行った。さらに、Android上で動作するプロトタイプもあわせて実装した。

具体的には、観測者による位置追跡から運転者のプライバシを保護するため、存在しないダミーの車の位置や速度を送信することで車の密度を増大させる手法を提案した。さらに、ダミーパケットによるノード密度の増大が位置追跡の成功率に与える効果を確認するため、シミュレーション評価も併せて実施した。

さらに本研究の根幹をなすプロトコル設計においては、まず通信方法と認証方法の検討を行い、効率の良い楕円曲線暗号（ECC）を選定し、ECCベースのセキュリティプロトコルの基本仕様の検討を進めた。これについては、CSS2012にて論文として発表を行った。

平成25年度

最終年度では、実機への実装と評価を念頭に研究を進めた。特に基盤となるITSアプリケーションが前提とするクロスレイヤモデルは、基本仕様が欧州等の標準化団体によって確固たるモデルが確定しており、それにあわせた設計が必要となる。そこで、その標準化されたプラットフォームに適した形で、より安全かつ効率の良いセキュリティプロトコルをECC上で構成されるペアリング暗号をベースとして設計を進めた。ペアリング暗号は、既存のRSA暗号と比較すると、有限体上および拡大体の計算構成上の都合から負荷が高くなることが分かっており、このためAndroidなどの計算リソースの限られたデバイス上で動作させるには、ある程度計算効率を考慮しておく必要がある。今回、高速化に着目した実装を行い、動作が可能なレベルまで実現することに成功した。具体的には、演算を構成するモジュールごとに効率化、および最適化を実施し、比較の上から適した値を設定することとした。本成果についてはSCIS2013にて論文発表を行っている。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 5 件）

1. 石井 将大，猪俣 敦夫，藤川 和利，Normal Basisを用いた多項式基底間の基底変換，FIT2013講演論文集 第1分冊，RA-006，pp.41-48，2013.
2. Satoru Noguchi, Satoshi Matsuura, Atsuo Inomata, Kazutoshi Fujikawa, Hideki Sunahara, Wide-Area Publish Subscribe Mobile Resource Discovery Based on IPv6 GeoNetworking, IEICE Transaction on Communication, E96-B, pp.1706-1715, 2013.
3. Satoru Noguchi, Atsuo Inomata, Kazutoshi Fujikawa, Hideki Sunahara, Design and field evaluation of geographical location-aware service discovery on IPv6 GeoNetworking for VANET, EURASIP Journal on Wireless Communications and Networking, Doi:10.1186/1687-1499-2012-29, 2012.
4. 猪俣 敦夫，岡本 栄司，攻撃能力見積もり手法，電子情報通信学会誌，20巻，pp.993-998，2011.
5. 池部 実，猪俣 敦夫，藤川 和利，広域分散環境におけるデータセマンティクスを用いた柔軟なデータシステムの提案と評価，日本ソフトウェア科学会論文誌，pp.93-104，2011.

〔学会発表〕（計　7　件）

1. Masahiro Ishii, Atsuo Inomata, Kazutoshi Fujikawa, Parallel GPU Implementation of \eta_T\ Oairing over Fields of Characteristic Two, 3rd International Conference on Network and Computer Science (ICNSC2014), 2014.
2. Tsubasa Teramoto, Satoshi Matsuura, Masatoshi Kakiuchi, Atsuo Inomata, Kazutoshi Fujikawa, Location Tracking Prevention with Dummy Messages for Vehicular Communications, 13th International Conference on ITS Telecommunications(ITST2013), 2013.
3. Yohei Kanemaru, Satoshi Matsuura, Masatoshi Kakiuchi, Satoru Noguchi, Atsuo Inomata, Kazutoshi Fujikawa, Vehicle Clustering Algorithm for Sharing Information on Traffic Congestion, 13th International Conference on ITS Telecommunications(ITST2013), 2013.
4. 石井将大、猪俣　敦夫、藤川　和利，種数 2 の超楕円曲線上に定義されたηT ペアリングの実装と標数 2 の有限体における離散対数問題，コンピュータセキュリティシンポジウム (CSS2013)，2013.
5. 瀬尾　奨太，猪俣　敦夫，櫨山　宏明，藤川和利，IP トレースバックダイジェスト手法における実攻撃を想定したフローダイジェスト方式の提案，情報処理学会コンピュータセキュリティ研究会（CSEC-56），2012.
6. Satoru Noguchi, Satoshi Matsuura, Atsuo Inomata, Kazutoshi Fujikawa, Location-aware service discovery on IPv6 GeoNetworking for VANET, 11th International Conference on Intelligent Transport System Telecommunications (ITST2011), 2011.
7. Noriaki Yoshikai, Ayako Komatsu, Atsuo Inomata, Experimental Research on Personal Awareness and Behavior for Information security Protection, International Conference of Network based Information Systems (NBiS2011), 2011.

〔図書〕（計　1　件）

1. 安岡寛道，曽根原登，吉井英樹，宍戸常寿，猪俣敦夫，東洋経済新報社，ビッグデータ時代のライフログ，2012，pp.52-56.

〔産業財産権〕
○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
猪俣　敦夫（INOMATA, Atsuo　　）
奈良先端科学技術大学院大学・総合情報基盤センター・准教授
研究者番号：90505869