様式 C-19

科学研究費補助金研究成果報告書

平成 21 年　6 月 12 日現在

研究種目：基盤研究(B)
研究期間：2006-2008
課題番号：18360185
研究課題名（和文）　利己的ノードを考慮した安全なモバイルアドホックネットワーク構成法の研究
研究課題名（英文）　A Secure Mobile Ad-hoc Network Configuration Method considering Selfish Nodes

研究代表者
高橋　修（TAKAHASHI OSAMU）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60381282

研究成果の概要：本研究では，モバイルアドホックネットワークにおける脅威として selfish ノードを前提に,移動機器で暗号方式を高速に実装するためのアルゴリズム,脅威の検出方式,回避方式などについて提案し，それらの有効性を実機，あるいは，シミュレーションにより実証評価した.

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	2,700,000	810,000	3,510,000
2007 年度	2,900,000	870,000	3,770,000
2008 年度	3,600,000	1,080,000	4,680,000
年度			
年度			
総　計	9,200,000	2,760,000	11,960,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：ネットワーク・LAN

１．研究開始当初の背景

(1)ネットワークが爆発的な勢いで我々の生活に普及していることに伴い，ネットワークセキュリティの脆弱性が社会問題となってきている．特に，ネットワークはモバイルアドホックネットワークへと進化してきており，セキュリティ問題も変化している.

(2)モバイルアドホックネットワークは無線電波を使用した移動機器で構成されているため，機器の電力，CPU 能力，通信能力の制約があること，管理者のいない不特定多数の移動機器でネットワークが構成されていること，移動機器は動いていること，などが特徴であり，従来の有線ネットワークのセキュリティ技術は，そのまま適用できない.

(3)具体的な例として，中継ノードとなるべき移動機器が自己消費電力の節約などを理由に，パケットの中継拒否や遮断を行う攻撃を行う（これらの移動機器を Selfish Node と呼ぶ）可能性があり，従来のネットワークでは存在しない新たなセキュリティ問題が発生する.

２．研究の目的

モバイルアドホックネットワークにおけるネットワーク構築．維持において，Selfish Node を考慮した安全で安心なサービス基盤技術を確立することを目標に，以下の研究・

開発を行うことを目的とし，以下の課題について検討する．
(1) 攻撃者(Selfish Node)の特定方式および排除方式の開発
(2) 再度チャネル攻撃(Node Capture)に対して安全な暗号/認証方式の開発
(3) 安全なモバイルアドホックネットワークのプラットフォームの開発と実証評価

３．研究の方法

本研究は，以下の方針で検討を進めた．最初に，種々の攻撃方法を分類整理するとともに，それらの検出方式について検討する．その後，提案方式をモバイルアドホックネットワークのシミュレータや移動機器に実装し，評価する．

このため，必要となる無線ホックネットワーク開発キットや PDA, およびシミュレータを動作させるためのパソコンなどの実験環境を整えた．

４．研究成果

研究成果を下記に示す．

(1)2006 年度の研究成果

主として，ペアリング暗号の高速実装とアドホックネットワークに対する攻撃に対する安全性の観点から検討を進めた．主な成果は以下の通りである．

① ペアリング暗号の高速実装

本研究では, 3 乗根を用いない η_T ペアリングの高速化アルゴリズム，およびトーラス T2 を用いた高速な最終冪のアルゴリズムを提案した．これらのアルゴリズムの改良により，GF(3^m)上の η_T ペアリングを約 25%高速化することが可能となった．

さらに，上記の提案改良アルゴリズムをソフトウェア実装した．その結果，計算時間は従来から報告されてきているペアリングのソフトウェア実装の中で最も高速に実現出来た．また， 携帯電話上にも実装し，実用的な時間で実装することが可能であることを示した．

これにより, ID ベース暗号やブロードキャスト暗号などペアリングを用いた新たな暗号応用技術が，携帯電話上のアプリケーションとして実現可能となった．

② ネットワークセキュリティ

最初に，モバイルアドホックネットワークのルーティングに関する脅威を体系的に分類するとともに，新しい攻撃方法である Ghost Attack を提案するとともにそのネットワークに与える影響を定量的に評価した．また，それに対する防御方式も提案し，攻撃を防げることもシミュレーションにより実証評価した．

また，最も甚大な被害を与えると予想されるブラックホール攻撃に対する防御方式を提案し，シミュレーションにより定量的に評価することによって，攻撃ノードを避けて安全に通信を継続出来ることを明らかにした．

(2)2007 年度の研究成果

2006 年度の成果をベースに以下の研究を進めた．

① ペアリング暗号を利用した高機能暗号プロトコルの構成

昨年度の成果である暗号ソフトウェアを利用して、ID ベース暗号、ショートシグネチャ、効率的なブロードキャスト暗号など、従来の暗号では実現できなかったセキュリティシステムを実装した．また、これらの暗号アプリケーションを、ユビキタス時代の大規模ネット向けのセキュリティ基盤に組込む研究も行った．

③ ネットワークセキュリティ

攻撃ノードが行いうる動作を網羅的に定義し，それらのノードが他のノードに与える影響を定性的・定量的に評価した．また，攻撃ノードの周辺ノードが攻撃ノードを高精度に検出する方式を検討した． さらに，あるノードが通信状況を周辺の他のノード（目撃者）から通信ログ（証拠）を収集することによって，後に紛争が発生した場合に自己の正当性を主張出来る証拠を収集する方式について検討した．また，効率良く情報を相手先まで配信するための経路構築や誤り制御方式などについても検討した．

(3)2008 年度の研究成果

以下の研究を進めた．

① ペアリング暗号を利用した高機能暗号プロトコルの構成

ユビキタスセンサーネットワークの要素技術として、ペアリング暗号を利用した暗号プロトコルとその高速実装を研究した。具体的には，センサーノード ATmega128L 上においてペアリング暗号の高速実装，公開鍵証明を利用しないハイブリット型の署名付暗号化方式の提案， RFID システムのタグとデータベース相互間の同期問題に関する考察を行った。

② ネットワークセキュリティ

モバイルアドホックネットワークのセキュリティに関して，攻撃ノードが行いうる動作を網羅的に定義し，その高精度な検出方式として，周辺ノードの目撃情報を利用する方式を提案し有効性を定量的に示すとともに，エンドーエンド間で効率良く情報を相手先まで配信するためにマルチパスを利用した経路構築方式とパケットスケジューリング方式，ネットワークコーディングによる誤り制御方式などについても検討した．

更に，インターネットの複雑な挙動をモデル化するために，適応的特徴空間構築方式を

提案し，多次元連続状態の強化学習に適用した．これにより，非線形関数を関数近似するための最適な特徴空間を構築できること，および環境の変化に応じて特徴空間を柔軟に再構築できることを示した．

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 10 件）

① Fagen Li, Masaaki Shirase, Tsuyoshi Takagi, Certificateless Hybrid Signcryption, The 5th Information Security Practice and Experience Conference (ISPEC 2009), LNCS 5451, Springer-Verlag, , pp.112-123, 2009（査読有）
② Hideki Sato, Reinforcement learning with orthonormal basis adaptation based on activity-oriented index allocation, IEICE Trans. Fundamentals, Vol. E91-A, No.4, pp.1169-1176, 2008（査読有）
③ 石黒司，白勢政明，高木剛，ATmega128L 上でのペアリング暗号の高速実装，情報処理学会論文誌，Vol.49，No.11，pp.3743-3753，2008（査読有）
④ 川原祐人，高木剛，岡本栄司，Java を利用した携帯電話上での Tate ペアリングの高速実装,情報処理学会論文誌,Vol.49, No.1，pp.427-435，2008（査読有）
⑤ Camille Vuillaume, Katsuyuki Okeya, Tsuyoshi Takagi, Short Memory Scalar Multiplication, IEEE Transactions on Computers, Vol.57, No.4, pp.481-489, 2008（査読有）
⑥ 横山信，高橋修，宮本衛市，アドホックネットワークにおける高精度な不正動作ノードの検出と防御方式の提案と実装評価,情報処理学会論文誌,Vol.49, No.2, pp.639-649，2008（査読有）
⑦ 高橋修，情報共有空間のためのモバイルアドホックネットワーク，情報処理学会誌，第 48 巻第 2 号，pp.154-159，2007（査読無）
⑧ 置田誠，山口典男，重松隆之，高橋修，宮本衛市，携帯電話機用 WEB ブラウザのサーバ・レンダリング方式の提案と実装評価，情報処理学会論文誌，第 47 巻第 7 号，pp.2107-2116,2006（査読有）
⑨ Hideki Satoh, Reinforcement learning for continuous stochastic actions --An approximation of probability density function by orthogonal wave function expansion --, IEICE Tans. Fundamentals, Vol. E89-A, no. 8, pp.2173-2180, 2006（査読有）
⑩ Hideki Satoh, A state space compression method based on multivariate analysis for reinforcement learning in high-dimensional continuous state spaces, IEICE Tans. Fundamentals, Vol. E89-A, no. 8, pp.2181-2191, 2006（査読有）

〔学会発表〕（計 29 件）

① 三科貴，高橋修，MANET フォレンジックスにおける証拠解析方式の提案,第 71 回情報処理学会全国大会，2009 年 3 月，滋賀県草津市
② 丹羽和弘,逢坂恭介,高木剛,高橋修，同期問題を考慮した安全な RFID 方式の提案，2009 年暗号と情報セキュリティシンポジウム（SCIS 2009），2009 年 1 月，滋賀県大津市
③ 森郁海，高橋修，アドホックネットワークにおける共通鍵共有方式の提案と実装・評価，情報処理学会 MBL 研究会，2009 年 1 月，北海道函館市
④ 森拓海，高橋修，アドホックネットワークにおける複数経路の利用による TCP/UDP 通信の性能向上の検討，情報処理学会 MBL 研究会，2009 年 1 月，北海道函館市
⑤ Akira Otaka, Tsuyoshi Takagi, Osamu Takahashi, Reliable Method for Collecting and Evaluating Transmission Records for MANET Forensics, 2nd International Workshop on Infomatics, IWIN 2008, September 2008, Wien, Austria
⑥ Akira Otaka, Tsuyoshi Takagi, Osamu Takahashi, Network Forensics on Mobile Ad-hoc Networks, 12th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, KES2008, September 2008, Zagreb, Croatia
⑦ 大高全，三科貴，高橋修，無線ネットワークにおける証拠の信頼性に関する一考察，平成 20 年電気学会電子・情報・システム部門全国大会，2008 年 8 月，北海道函館市
⑧ 高橋修，アドホックネットワークにおけるセキュリティ，電子情報通信学会アドホックネットワーク研究会,2008 年 7 月，北海道函館市
⑨ 森郁海，森拓海，小野良司，撫中達司，高橋修，アドホックネットワーク(VANET,MANET)におけるセキュリティの定性評価とセキュアルーティングプロトコルの現状と課題，情報処理学会 DICOMO2008 シンポジウム，2008 年 7 月，

北海道札幌市

⑩ 森拓海，森郁海，小野良司，撫中達司，高橋修，アドホックネットワーク(VANET, MANET)のセキュリティ評価項目の明確化とセキュリティ要素の相互補完可能性の検討，情報処理学会 DICOMO2008 シンポジウム，2008 年 7 月，北海道札幌市

⑪ K.Sekiguchi，S.Imai，Y.Yamamoto，N.Meuchi，O.Takahashi，Evaluation of Flight Size Auto Tuning on 3.5G Commercial Wireless Packet Access Network，The 23rd International Technical Conference on Circuits/Systems，Computers and Communications (ITC-CSCC2008)，July，2008，福岡県北九州市

⑫ K.Sekiguchi，S.Imai，Y.Yamamoto，N.Meuchi，O.Takahashi，Implementation and Evaluation of TCP Retransmission Algorithm For Wireless Packet Channel with Delay Variation，International Conference on Mobile Computing and Ubiquitous Networking (ICMU2008)，June，2008，東京

⑬ 森郁海，高橋修，ビザンチン攻撃の検出と回避を考慮した Hop By Hop ベースルーティングプロトコルの提案と実装・評価，情報処理学会第 45 回モバイルコンピューティングとユビキタス通信研究会，2008 年 5 月，沖縄県那覇市

⑭ 森拓海，高橋修，Hop by Hop ルーティングプロトコルにおけるノードディスジョインとな経路構築報の検討・評価，情報処理学会第 45 回モバイルコンピューティングとユビキタス通信研究会，2008 年 5 月，沖縄県那覇市

⑮ Kyosuke Osaka，Shuang Chang，Tsuyoshi Takagi，Kenichi Yamazaki，Osamu Takahashi，A Secure RFID Protocol based on Insubvertible Encryption using Guardian Proxy，The Third International Conference on Availability，Reliability and Security，ARES 2008，March,2008，BARCELONA，SPAIN

⑯ 大高全、高橋修，MANET におけるフォレンジクス技術適用に関する提案，情報処理学会 MBL 研究会，2008 年 3 月，東京

⑰ 片山貴充，高木剛，アクセス制限可能なキーワード検索可能暗号方式，暗号と情報セキュリティシンポジウム，SCIS 2008，2008 年 1 月，宮崎県宮崎市

⑱ 石黒司，白勢政明，高木剛，ATmega128L 上でのペアリング暗号の高速実装，情報処理学会 コンピュータセキュリティシンポジウム，CSS 2007，2007 年 10 月，奈良新公会堂（奈良県）

⑲ 仁科五月，高木剛，Window 法による有限体 GF(p^m)の高速演算法の解析，情報処理学会 コンピュータセキュリティシンポジウム，CSS 2007，2007 年 10 月，奈良新公会堂（奈良県）

⑳ 山田尚志，高木剛，櫻井幸一，2 冪算における直接計算法を用いたマルチスカラー倍算の効率性評価，電子情報通信学会，情報セキュリティ研究会，2007 年 9 月，東京

㉑ Hideki Satoh，Linearization and Approximate Optimal Control for Non-linear Systems Based on MVE and LQ Control，36th SICE Symposium on Control Theory，2007 年 9 月，北海道札幌市

㉒ Motoi Yoshitomi，Tsuyoshi Takagi，Shinsaku Kiyomoto，Toshiaki Tanaka，Efficient Implementation of the Pairing on Mobilephones using BREW，The 8th International Workshop on Information Security Applications，WISA 2007，Aug，2007，Jeju Island，Korea

㉓ 森郁海，森拓海，高橋修，AODV ベースセキュアルーティングプロトコルの提案とその実装・評価，情報処理学会 DICOMO シンポジウム，2007 年 7 月，三重県鳥羽

㉔ 森拓海，森郁海，高橋修，AAAr: Anti Attack Ad-hoc routing protocol の提案と実装・評価，情報処理学会 DICOMO シンポジウム，2007 年 7 月，三重県鳥羽

㉕ 森郁海，森拓海，高橋修，アドホックネットワークにおける攻撃法・防御法の分類と AODV ベースセキュアルーティングプロトコルの提案，情報処理学会，MBL 研究会，2007 年 5 月，沖縄県那覇市

㉖ 森拓海，森郁海，高橋修，アドホックネットワークにおける防御法の分類と耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャの提案，情報処理学会，MBL 研究会，2007 年 5 月，沖縄県那覇市

㉗ Eun-Kyung Ryu，Tsuyoshi Takagi，Efficient Conjunctive Keyword-Searchable Encryption，3rd IEEE International Symposium on Security in Networks and Distributed Systems，SSNDS 2007，May，2007，Niagara，Canada

㉘ 森郁海，横山信，高木剛，山崎憲一，高橋修，アドホックネットワークにおけるブラックホール攻撃に対する防御法の提案と実装・評価，情報処理学会研究報告，Vol. 2006，No.120，pp.47-52,2006　広島県広島市

㉙ 森拓海，横山信，高木剛，山崎憲一，高

橋修, AODV における Ghost Attack とその防御法, 情報処理学会研究報告, Vol. 2006, No.120, pp.53-58,2006 広島県広島市

〔図書〕（計１件）

① Kyosuke Osaka, Tsuyoshi Takagi, Kenichi Yamasaki, Osamu Takahashi, Springer-Verlag, RFID Security: Techniques, Protocols and System-on-Chip Design, 2008, 443

６．研究組織

(1)研究代表者

高橋　修（TAKAHASHI OSAMU）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60381282

(2)研究分担者

佐藤　仁樹（SATO HIDEKI）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：30360001
高木　剛（TAKAGI TSYYOSHI）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60404802

(3)連携研究者