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　１０日現在

研究種目：基盤研究（Ｂ）
研究期間：2007～2009
課題番号：１９３６０１７６
研究課題名（和文）　非線形的アプローチによる大規模システムの制御とセキュアネットワークへの応用
研究課題名（英文）　Control of Large Scale Systems and its Application to Secure Network Based on Nonlinear Approach

研究代表者
佐藤　仁樹（SATOH 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

研究成果の概要（和文）：本研究では、多変量解析、フーリエ解析、強化学習などの数理科学的な手法を用いた大規模非線形システムの制御方式、セキュアな通信方式、および盗聴を防ぐためのペアリング暗号方式を提案した。また、これらの提案手法を、セキュアネットワークに関する課題に適用した。その結果、従来は不可能だった角度から、様々な通信ネットワークの安全性を検証し、通信ネットワークのセキュリティを向上させることができた。

研究成果の概要（英文）：Secure communication systems, pairing encryption, and control methods of large-scale nonlinear systems based on mathematical science such as multivariate analysis, Fourier analysis, and reinforcement learning were developed. These methods were applied to various problems in secure networks. We could evaluate the reliability of various types of networks and improve network security.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	4,200,000	1,260,000	5,460,000
2008 年度	3,600,000	1,080,000	4,680,000
2009 年度	3,000,000	900,000	3,900,000
年度			
年度			
総　計	10,800,000	3,240,000	14,040,000

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：数理科学、セキュア・ネットワーク、暗号、認証、機械学習、非線形科学

１．研究開始当初の背景

(1) セキュアネットワークの必要性と課題

通信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現状にともない、不正アクセス、コンピュータウイルス、プライバシー侵害、フィッシング詐欺など、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。日々新たなセキュリティ被害が報告されているのが現状であり、今後この傾向が収束すると予想している研究者は皆無であ

る。また通信ネットワークは、モバイルアドホックネットワークという形に進化しており、それに伴いセキュリティ問題も変化している。

モバイルネットワークのセキュリティ研究は、アドホックネットワークの物理レイヤでの盗聴を困難にする通信方式やデバイス認証方式、無線LANの暗号/認証方式、モバイルネットワークにおけるAAAなど、暗号化技術、認証技術の研究が殆どであった。一方、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モバイル機器で構成されるため、従来の通信ネットワークとの大きく異なる特徴を持つ。さらに、ノードの消費計算時間等を正確に計測することにより暗号を破るサイドチャンネル攻撃のような新たな攻撃が次々と発生している。このため、従来の通信ネットワークで使用されてきた伝統的なセキュリティ技術はそのまま適用できない。

(2) セキュアネットワーク実現に対する障害

現代の通信ネットワークは、前述のように様々な危機に直面しており、その課題の解決は急務である。しかしながら、これらの課題を本質的に解決することは、以下の理由により非常に困難である。

・通信ネットワークの多様性：インターネットに代表される現代の通信ネットワークは、非常に多くのノードや端末から構成されている。また、ネットワーク構造、制御方式、通信方式などが多様化している。

・大規模かつ非線形性：従って、全世界の通信ネットワークが一つの巨大な非線形システムとなっており、システム全体をモデル化できない。

・理論展開の困難さ：そのため、数理科学的な手法を用いて、矛盾のない理論展開により特性解析手法や制御方式を検討できない。

従って、通信ネットワークのごく一部の状態や特性に着目した対処療法的な解決策しか見いだせない。

⑶ 非線形問題解決のための従来手法

非線形問題を解決する代表的な方法として、ガレルキン法、摂動法、漸近法が上げられる。これらの方法により、微分方程式や偏微分方程式で記述された非線形システムの解を近似的に求めることができる。また、平均値近傍における線形化により、システムの安定性を調べることができる。しかし、これらの手法には以下のような限界があった。

・本研究が対象としているインターネット、アドホックネットワーク、モバイルネットワークは、非常に多くのノードや端末から構成されている。そのため、従来の方法で解を求めることは困難である。また、仮に解が求まったとしても、非常に複雑な式になることは明らかである。

・実際に必要な情報は、平均、分散、パワースペクトラムなどの統計情報や、制御入力に対する過渡応答などであり、これらは近似解から直接得られない。従って、近似解を求める手法により、通信ネットワークの性質や、適切な制御入力を決めることは困難である。

・平均値近傍での線形化により、インターネットトラヒックの安定性を調べた研究がある。しかし、このモデルは適用範囲が狭いため、一般的な性質の解析や、通信ネットワークの制御に用いることは困難である。

そのため、現代の通信ネットワークが直面している様々な危機を本質的に解決するためには、従来とは異なる新しいアプローチが必要である。

２．研究の目的

セキュアネットワーク実現に対する課題を解決し、非線形的なアプローチにより実社会のシステムを構築するための学術的な基礎を構築することを目的とする。詳細は以下の通りである。

(1)非線形モデルの構築－制御空間の圧縮－

様々な形態の通信ネットワークに適用できるセキュアルーチング技術を構築するために、ルーチングテーブルの制御空間を圧縮するための非線形モデルに、ノード数、ネットワークトポロジー、電波伝搬路、端末の移動などの状況をパラメータとして導入する。さらに、暗号評価のための非線形モデル、および攻撃パターン同定のための非線形モデルを構築する。

(2) 大規模非線形システムの解析および制御

大規模非線形システムの制御方式の収束速度を改善し、想定される通信ネットワークの変動（端末の移動、トラヒックの変動）に追従できる制御方式を提案する。

(3) ネットワークセキュリティ技術の構築

前述の非線形モデルおよび制御方式を用いて、セキュアネットワーク実現に必要となる３つの技術（セキュアルーチング、サイドチャンネル攻撃に対する暗号方式の評価、攻撃者および攻撃パターンの同定）を構築する。

３．研究の方法

セキュアネットワーク実現に必要となる技術を非線形的アプローチにより構築するために、2007年度は、大規模非線形システムの解析および制御方式の構築、およびセキュアネットワークに必要な非線形モデルの構築を中心に研究を進めた。本研究により、非線形問題を解決するための様々な手法を、セキュアネットワークの課題に適用するための基礎を

構築した。2008年度は、2007年度に引き続き、セキュアネットワークに必要な非線形モデルを構築する。2009年度は、2007～2008年度に得られた成果を元に、セキュアネットワークを実現するために、攻撃者および攻撃パターンの同定、サイドチャンネル攻撃に対する暗号方式の評価、セキュアルーチングに関する課題を解決した。

本研究の目的は、セキュアネットワーク実現に対する課題の解決である。そのため、提案された手法の評価には、実際のネットワークを想定した多くのシミュレーションを実施しなければならない。そこで、補助金により高速な計算機を購入し、膨大な計算が必要となるこれらのシミュレーションを実施した。

４．研究成果

(1) ルーチングのための非線形モデルと制御方式

研究代表者が提案した強化学習に基づくロバストルーチング方式(雑誌論文⑥)の収束速度を改善するために、モーメントベクトル方程式を用いて非線形システムを定義域全体で線形近似し、線形システムの代表的制御手法である線形２次評価関数に対する解法により制御関数を導く方法を提案した(雑誌論文②)。簡単な１次元双線形システムに対して本手法を適用し、本手法により近似的な最適制御が得られることを確認した。

(2) セキュアルーチング

研究代表者の佐藤は、多変量解析に基づく状態空間の圧縮方式、非線形関数を関数近似するための特徴空間構築方式、及び探索空間を圧縮するためのポテンシャルモデルを導入し、強化学習に基づくロバストルーチング方式を提案した(雑誌論文⑥)。さらに、予備制御器から得られた行動の主成分分析に基づき、高次元行動空間を圧縮する方法を提案した(学会発表⑩)。提案されたアルゴリズムは、ネットワークの全ての状態を考慮し、有効でない情報を排除することができる。そのため、ルーチングループや局所最適解に陥る頻度を削減し、効率の良いルーチングテーブルを作成できる。さらに、ルーチング情報が妨害された場合でも、良好に動作する。詳細なシミュレーションにより、提案したルーチング方式が、従来手法に比べて様々な攻撃パターンに柔軟に対応できることを示した。

(3) 最適解探索手法

研究代表者の佐藤は、本研究課題により得られた様々な研究成果を統合し、セキュアルーチング方式を実用化するための技術を提案した。まず、多くの要素の結合系システムをモーメントベクトル方程式で近似し、その特性を解析する手法を提案した(学会発表③)。本手法はシミュレーションでは検出困難な状態を検出できるという特徴を持つため、ネットワークの状態を解析するだけでなくセキュリティホールの発見にも有効である。次に、ルーチング問題などの大域的最適化問題がシュレディンガー型方程式のハミルトニアンの固有値問題と等価になることを示し、大域的最適解を必ず求められる方法を提案した(雑誌論文①,学会発表①)。本手法は従来とは異なる新しい最適化手法であり、最適なルートを探索するために有効である。さらに、多数の時系列データから有効な特徴を抽出し、非線形時系列の変動を予測する方式を開発した(学会発表②)。本手法により、多地点から収集したトラヒックデータを有効に利用し、ネットワークの振る舞いを予測できる。

(4) 攻撃パターンの同定とセキュア通信環境

信頼関係のないアドホックネットワーク環境でのセキュア通信環境基盤のための基礎技術を確立した。まず、攻撃ノードの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(雑誌論文⑦)。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(雑誌論文⑦)、通信状況を周辺の他のノードから収集し、自己の正当性を主張する方式(学会発表⑤,⑮)、および、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(学会発表④,⑦)を提案した。

(5) セキュア通信プロトコル

セキュアネットワークの要素技術として、信頼性を確保するためにNetwork Codingを利用したパケット転送方式(雑誌論文④,学会発表⑥,⑫)、無線ネットワークにおけるスループットを向上するためのTCPの再送方式(学会発表⑧,⑬)、および複数のルートを使ったパケット転送方式(学会発表⑭)を提案した。これらにより、ネットワークに対する攻撃やパケット廃棄が頻繁に発生する無線ネットワークにおいて、データを高信頼かつ高効率で送信するためのネットワーク基盤技術を確立した。

(6) セキュアネットワークのための暗号技術

ペアリング暗号は、 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構成できる。本研究では、ペアリング暗号で必要となるアルゴリズム基礎部分の暗号ライブラリを実装し、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技術を開発した(雑誌論文⑧,学会発表⑲)。また、大規模なセキュアネットワークの要素技術として、標数３の有限体に対するリダクションが高速となる既約多項式

を提案(雑誌論文⑤)、スカラー倍算の高速実装を実現した(学会発表⑰,⑱)。 また、高速化が望まれる超楕円曲線上のペアリング暗号を実装し、その有効性を示した(学会発表⑨,⑪)。 さらに、要素技術である暗号技術を評価するために、素体上の超特異 楕円曲線におけるペアリン グ暗号の高速実装アルゴリズムを構成した(雑誌論文③)。また、RFIDのセキュリティ方式における距離制限プロトコルを考察し、フォワードセキュアな方式を提案した(学会発表⑯,⑳)。

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９件）

① H. Satoh、Global Nonlinear Optimization Based on Wave Function and Wave Coefficient Equation、IEICE Trans. Fundamentals、査読有、Vol,E93-A、No.1、2010、pp,291-301、
② H. Satoh、Moment Vector Equation for Nonlinear Systems and Its Application to Optimal Control、IEICE Trans. Fundamentals、査読有、Vol.E92-A、No.10、2009、pp.2522-2530、
③ 中島俊哉、伊豆哲也、高木剛、素体上の超特異楕円曲線におけるペアリング暗号の効率的な計算手法、情報処理学会論文誌、査読有、Vol.50、No.7、2009、pp.1745-1756、
④ T. Kagi、O. Takahashi、Determining the Relay Node Encode Packet in Multipath Routing Environment、 Int. J. Infomatics Society、査読有、Vol.1、No.2、2009、pp.12-18、
⑤ T. Nakajima、T. Izu、T.Takagi、Reduction Optimal Trinomials for Efficient Software Implementation of the EtaT Pairing、IEICE Trans. Fundamentals、査読有、Vol,E91-A、No.9、2008、pp.2379-2386、
⑥ H. Satoh、A nonlinear approach to robust routing based on reinforcement learning with state space compression and adaptive basis construction、IEICE Trans. Fundamentals、査読有、Vol.E91-A、No.7、2008、pp.1734-1740、
⑦ 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、査読有、Vol.49、No.2、2008、pp.639-649、
⑧ 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、査読有、Vol.49、No.1、2008、pp.427-435、

〔学会発表〕（計３７件）

① H. Satoh、Schrodinger-type Equation for Nonlinear Optimization and its Application to Global Optimization、IEICE Technical Report NLP2009、pp.21-26、Dec. 21, 2009、岩手県盛岡市清温荘、
② 高岩麦、佐藤仁樹、強化学習を用いた高次元非線形時系列予測、IEICE Technical Report NLP2009、pp. 37-42、2009年12月21日、岩手県盛岡市清温荘、
③ H. Satoh、Analysis Based on Moment Vector Equation for a Many-body System with Linear Interactions、IEICE Technical Report NLP2009、pp.197-202、2009年11月14日、鹿児島県屋久島環境文化センター、
④ H. Narumi、Y. Shiraishi、O. Takahashi、A Proposal of Reliable Cluster-by-Cluster Routing Method in MANET and its Evaluation、International Workshop on Infomatics 2009、Sept. 14, 2009、Hawai(U.S.) Hawai Tokai International College、
⑤ 三科貴、大高全、白石陽、高橋修、MANETフォレンジクスにおける Bloom Filterによる効率的な証拠解析手法、情処学会DICOMO2009、pp.815-822、2009年7月8日、大分県別府市 杉乃井ホテル、
⑥ 大竹健司、高橋修、白石陽、ネットワークコーディングを用いた ALMにおけるノード離脱を考慮した経路構築法の提案と評価、情処学会DICOMO2009、pp.107-113、2009年7月8日、大分県別府市杉乃井ホテル、
⑦ 鳴海寛之、白石陽、高橋修、Cluster-by-Cluster ルーティングにおけるクラスタヘッド選出手法に関する検討、情処学会DICOMO2009、pp.1074-1083、2009年7月8日、大分県別府市 杉乃井ホテル、
⑧ 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、情処学会研究報告2009-MBL-48、pp.33-40、2009年1月29日、北海道はこだて未来大学、
⑨ 古林靖規、高木剛、素体上の大きな種数を持つ超楕円曲線上のペアリング暗号実装、2009年暗号と情報セキュリティシンポジウム、SCIS 2009、4C1-1、2009年1月20日、滋賀県大津プリンスホテル、
⑩ H. Satoh、Reinforcement Learning for High-dimensional Action Space -- Action Space Compression Based on Principal Component Analysis --、IEICE Technical Report NLP2008-64、pp. 37--42、Nov.6, 2008、愛知県名古屋大学、
⑪ 古林靖規、高木剛、種数の大きな超楕円曲線を利用したTateペアリングの実装、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 2008、pp.187-192、2008年10月8日、沖縄県沖縄コンベンションセンター
⑫ T. Kagi、O. Takahashi、Efficient Reliable Data Transmission using Network Coding in MANET Multipath Routing Environment、12th International Conference、KES2008、PartIII、LNAI5179、pp.183-192、Sept. 3, 2008、Zagreb, Croatia、
⑬ K. Sekiguchi、S. Imai、Y. Yamamoto、N. Meuchi、O. Takahashi、Evaluation of Flight Size Auto Tuning on 3.5G Commercial Wireless Packet Access Network 、Proceedings of 23rd International Technical Conference on Circuits/Systems、Computers and Communications（ITC-CSCC2008）、pp.489-492、July 6, 2008、福岡県海峡メッセ下関、
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トな経路構築法の検討、評価、情報処理学会研究報告、2008-MBL-45、pp. 135-140、2008年5月17日、沖縄県青年会館、
⑮ 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5日、東京都慶応大学、
⑯ 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22日、宮崎県フェニックス・シーガイア・リゾート、
⑰ 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12月19日、東京都機械振興会館、
⑱ 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31日、奈良県奈良新公会堂、
⑲ M. Yoshitomi、T. Takagi、S. Kiyomoto、T. Tanaka、Efficient Implementation of the Pairing on Mobilephones using BREW、The 8th International Workshop on Information Security Applications、WISA 2007、Aug. 27, 2007、Jeju Island、Korea、
⑳ E. Ryu、T. Takagi、Efficient Conjunctive Keyword-Searchable Encryption、3rd IEEE International Symposium on Security in Networks and Distributed Systems、SSNDS 2007、May 21, 2007、Niagara, Canada、

６．研究組織

(1)研究代表者
佐藤　仁樹　（SATOH　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

(2)研究分担者
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

高木　剛　（TAKAGI　TSUYOSHI）
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