様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１２　日現在

機関番号：　８２７２３
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2016
課題番号：　２４５６０４９１

研究課題名（和文）ネットワーク符号化の応用によるセキュアパケット・ルーティングに関する先駆的研究

研究課題名（英文）Research on secure packet/routing on network coding

研究代表者

田中　秀磨（Tanaka, Hidema）

防衛大学校（総合教育学群、人文社会科学群、応用科学群、電気情報学群及びシステム工・電気情報学群・准教授

研究者番号：３０３２８５７０

交付決定額（研究期間全体）：（直接経費）　　4,000,000円

研究成果の概要（和文）：本研究はネットワーク符号化を用いた通信においてセキュアなパケット構成とルーティングに関するものである。成果として①代数的手法の応用、②脅威/安全性の定量化、③新たな攻撃手法の模索、④ユーザの権利確保とプロトコルの提案、があげられる。当初の目的である実機による評価実験は運営上の理由により行えなかったが、各サブテーマで発展的な成果を挙げることができた。主にブロック暗号の新たな安全性評価手法、離散フーリエ変換を用いて定量化された攻撃検知手法、Slow Read DoS攻撃の攻撃効果改善手法が挙げられる。

研究成果の概要（英文）：In this research activity, our purpose is to derive the secure construction method for packet and routing method for network service using network-coding. As the results, we can get following outcomes; 1) algebraic method for security applications, 2) quantification method for threat/security, 3) development of new attack method, and 4) user's right and secure protocol. Though evaluation experiments using real network environment is the first purpose, we could not be available because of the operation-rule, however we could develop many outcomes by each sub-theme. For example, new evaluation methods for block ciphers, quantified intrusion detection system using discreet Fourier transform, and improvement of Slow Read DoS attack.

研究分野：　情報セキュリティ

キーワード：　ネットワーク符号化　ブロック暗号　代数的手法　攻撃検知　固有値　プライバシー

１．研究開始当初の背景

ネットワーク符号化技術は、通信路の途中に存在するノードも演算処理を行うことを前提としたもので、従来の符号化を用いた通信よりも同じ帯域幅で送信できる情報量が増大し、通信効率を向上できる。この技術をネットワーク構築に応用した顕著な例として、SDN(Software Defined Network)や Open Flow Network がある。また広義の解釈ではあるが、MIMO(Multi-Input Multi-Output)もネットワーク符号化技術の応用の一つと捉えることもでき、各種無線通信の効率の向上にも貢献できる。

物理的に構築するネットワークにおいては、各ノードが全てのノードに接続している形態(フルメッシュ接続)を前提とし、ネットワークの管理サーバが別途必要となる。このため従来のネットワーク構築に比べ運営・導入コストが上がることが大きな欠点として指摘されている。さらにノードが不正な処理を行う、勝手に別のノードとの通信を行う、などセキュリティ上の問題もあるが、あまり大きな欠点としては指摘されてこなかった。これは運営側を信用することを前提とする考え方が一般的であることが原因である。また、ネットワークが、通信する対象のコンテンツに応じて、その形態を変化させ、それぞれの目的に合わせた通信効率の向上を可能にできる一方で、通信内容の暴露などユーザのプライバシー問題への発展も指摘されている。

このようにネットワーク符号化をネットワーク構築に導入することは、従来よりも通信効率の向上や利便性の改善が期待でき、さらには災害時などにおける通信遮断の回避など、実利点が多い。しかしながら、導入に関する高コスト化は別として、ユーザ視点では従来のネットワーク利用よりも、セキュリティや運営に対する信用という点で前提とすべき条件が多く、新たな問題の生起も大きいと言えた。しかしながら、応募時点と比較して現状では、ユーザ意識の変化が大きいと考えられるが、これらはあまり指摘されず利用・普及の拡大一途である。また、主に産業界における標準化により、セキュリティの仕組みがあまり公にされないまま、例えばクラウドストレージなどでユーザ数及び利用データ量は劇的に増加している。

２．研究の目的

本研究では、ネットワーク符号化技術において、ユーザの権利を守る目的で、セキュアなルーティング及びパケット構成に関して新提案を行い、実験的な実ネットワーク環境を構築した上で評価することを目的とした。この点で、上述のようにユーザは運営側を無条件に信用しておらず、ユーザの権利が守られていることを確認できる手法の確立を目的としていた。しかしながら、応募者の事情ではあるが、応募時と採択時で所属機関を移籍したため、実験環境の構築に苦慮し、また、職務上の新たな役割などから大幅な変更をせざるを得なかった。結果的に平成 26 年度(3年目)の時点で方針転換を決断した。そのため、平成 26 年前後で少々趣旨の異なる内容となってしまったが、基本的には大きな 2 つ目的からは外れていない。すなわち 1)ユーザの権利を犯す新たな手段とその検知、2)ユーザのプライバシーを保護するプロトコルの提案、である。

1)は、セキュアなパケット構造の提案に繋がるが、前述のように実験環境が不備であること、既に標準化が進み利用が拡大し新規提案の意義が薄れたことから、新たな脅威の模索とその対策の必要性に重点を置き、合わせて既存のセキュリティ技術の安全性評価手法への応用を行うこととした。

2)はセキュアなルーティングに関する研究となるが、上述と同様の理由により、新たな攻撃シナリオの模索に位置付けた。特にネットワーク構造を意図的に改変し、攻撃に都合の良い攻撃戦略の策定に取り組むこととした。同時に攻撃がネットワークの効率性に直接影響を与えず、ユーザに被害を与える手段について、その攻撃効率の向上を行うことで対策手法の導出を目的とした。

これらに加えて、3)ユーザの権利確保のため、主に情報倫理の分野から取り組みを行う事とした。従って、応募時の主テーマである

1)セキュアパケットの構成
2)セキュアルーティングの導出
3)ユーザの権利確保

の目的から、大きくはずれていないものの、達成すべきゴールは大きく修正した。

３．研究の方法

応募時に想定していた研究体制では、国内外の研究者を招聘し、各テーマでグループを構築する予定であった。特にネットワーク符号化におけるパケット構成では、中国・ロシアの研究者招聘を予定していたが、移籍後にはこのような体制による活動が難しくなり、断念せざるを得なかった。また想定していた参画研究者も所属が変更になったので、研究分担者/連携研究者としての設定ではなく、通常の共同研究者扱いとなった。一方で、移籍後は大学院生クラスの学生を担当することとなったので、彼らの職務研究テーマと一致できる範囲で、本研究テーマを盛り込み遂行することとした。従って、日本人学生 4 名、留学生 2 名(韓国、モンゴル)の計 6 名と、千葉大/東京芸術大及び情報通信研究機構から各 1 名ずつの合計 8 名との共同研究という形式をとった。

前述のように、大幅な方針転換を行なったが、研究目的を細分すると以下の 4 つのテーマに分類できる。

①代数的手法の応用
②脅威/安全性の定量化
③新たな攻撃手法の模索

④ユーザの権利確保とプロトコルの提案
①〜③は応募者が主となり、それぞれ学生との共同研究を行なった。④は主に千葉大/東京芸術大及び情報通信研究機構との共同研究であり、応募者のアイデアについて情報倫理的な解釈及び評価を担当していただいた。前述の主テーマとの関連は以下の通りである。

1)セキュアパケットの構成 → (1)(2)
2)セキュアルーティングの導出 → (3)
3)ユーザの権利確保 → (4)

本分類に基づいて研究成果を述べる。

４．研究成果

(1)代数的手法の応用

ネットワーク符号の構成は代数的処理を基にしており、符号化/復号が可能である必要があることから一対一関数として定義される。この一対一関係は、符号の構成だけでなく利用する暗号化処理にも適用することで、復号することなく、暗号文に処理を施しながら情報を上書きすることが可能となる。しかしながら一対一関数をそのまま暗号化処理に適用すると全く安全性を実現できない。そこで比較的構成が単純で、一対一関数を大量に利用することを基本としている軽量ブロック暗号の応用を考えた。

結果的にはむしろこのような一対一性に注目することで安全性を覆す攻撃手法の提案に行き着いた。本来の目的では、符号の構成法への応用を考えていたが、以下の新たな問題の解決が必要となった。

課題 1)処理を部分構成に分解すると特定の入出力関係で一対一関係が成立し、安全性を実現できない(選択平文攻撃)。どのように入力を選ぶと攻撃者有利となるのかを探索する必要ができてきた。

課題 2)一対一関係を効率よく積み重ねることで暗号化処理全体の安全性を引き下げることができることを発見した(代数的特性の特定)。

課題 3)一対一関係を安全にするためには代数次数を大きくすることが基本となるが、どの程度大きいのかを評価する手法は、基本的には代数関係式の展開を行うしかない。しかしながら、この手法では探索範囲が非常に限られる上に正確な見積もりが難しい。

課題 1 に対してはインテグラル攻撃を中心に、その攻撃に対して有効な平文選択法を提案した。いくつかの暗号方式に対して適用した結果は、従来のものと同等であり、既存見積もりが正しいことを裏付けた。また、必要な計算量が小さく、計算時間も従来手法よりも短い結果となった。課題 2 に関しては、一般的にトレイル探索と呼ばれる手法であり、従来は全数探索が中心であった。本研究では特性間の繋がりをあらかじめ表として記憶しておき、GPGPU を用いて探索する手法を提案した。その結果、従来手法では発見できなかった別のトレイルを発見した。このような別のトレイルを用いると暗号系全体の攻撃を行う上で必要なデータ量の削減に有効であることを示した。課題 3 に関しては、前述のように代数展開式を求めることで達成できるが、入力のサイズが大きいと計算機探索が不能となる。例えば 128[bit]入力であれば、項数が 10^{43} 個程度となり現在のスーパーコンピュータでも処理は不可能となる。本研究では、ランダムに処理途中の項を選び、それだけの試行を行うことで計算量を削減し、下限のみを示す手法を提案した。

以上の手法は、そのままネットワーク符号化されたデータからセキュアなパケットを生成するための要素技術となり得ると期待している。具体的なパケット構成に関してはアイデアレベルに留まり、引き続き研究を継続する予定である。

(2)脅威/安全性の定量化

ネットワークにおける攻撃の検知には、大きく 2 通り存在する。一つはこれまでの攻撃結果を用いて、それに合致する特徴を持つ通信を攻撃として検知するもの(シグニチャタイプ)。もう一つは通信の振る舞いから異常を検知する手法(アノマリタイプ)。前者は確定的に攻撃を検知できるが新種攻撃を見逃す可能性が高い。一方、後者は新種攻撃を見つけることができるものの、通常の通信も異常と誤検知する問題が指摘されている。

本研究では後者のタイプに注目し、異常を定量的に評価する手法に関して取り組んだ。このために、通常と異常の差をシャノン=ハートレーの定理を用いてエントロピーで評価する方法を提案した。本手法では時間変化分に対して離散フーリエ変換を適用することでスペクトラム解析を行い、そのエントロピーを求めた。公開されている評価用通信ログデータである Kyoto2006+を用いて提案手法を適用したところ、概ね 90%程度で異常を検知できることが分かった。

本手法の利点は、他の手法は例えば機械学習などを用いるため検知のための処理時間や教師データが必要になるのに対し、異常を判別するエントロピーの閾値だけを利用する点にある。そのためシステムに対する要求性能が小さく、データベースも必要としない。また離散フーリエ変換の計算自体も軽い処理のため、例えば組織全体の通信に対してフィルタを利用して選別せず、全ての監視が可能である。しかしながら 90%の検知は攻撃検知システムとして見た場合、低い検知能力と言わざるを得ない。誤検知の大部分は通常を異常と判断する誤検知であった。そこで、前述のように処理の軽さを生かし、他の攻撃検知システムの前に判断させるプロアクティブ使用を提案した。

ところで、このような離散フーリエ変換を用いてエントロピーで異常を検知する手法は他のセキュリティ問題にも応用が可能である。本研究では、暗号技術が実装されてい

る暗号モジュールの安全性評価に応用した。暗号モジュールはその動作時に消費電力波形、漏洩電磁波など物理現象という形で内部の処理状態を漏らす。このような物理現象を用いた攻撃手法をサイドチャネル攻撃と呼ぶ。様々な対策手法が提案されているが、その効果は実際に攻撃試行することで評価されている。本提案手法を適用すれば、エントロピーで安全性を評価し、攻撃が成立するか否かを確定的に判断できる。ストリーム暗号 Enocoro-V2 を実装した FPGA ボードを対象に評価を行い、有効性を示した。また、本手法の基本アイデアは量子雑音を利用した暗号系に対する安全性評価であり、これも本研究成果の一つとして挙げた。

以上のように、本課題はパケットが持つ安全性評価を定量的に行う手法へと展開が可能である。

(3)新たな攻撃手法の模索

前述の(2)とも関連するが、セキュアなルーティングを提案するためには、新たな攻撃シナリオを事前に設定しなければならない。本研究では 2 種類の異なるアプローチをとった。

1)ネットワーク全体を攻撃対象とし、どのノードを攻撃するのが最も適切か、を探索する。ネットワークの形状を変えることで攻撃者有利な状況を作り出す。具体的な攻撃手法は設定しない。

2)できるだけネットワークの形状を変えないで、特定のノードだけをダウンさせる。この結果、有効なルーティングが行えず通信効率が落ちる。

1)の手法として、ネットワーク全体を接続行列及びラプラシアン行列で表現し、その固有値が攻撃の結果どのように変化するかで、攻撃の有効性を評価する手法を提案した。攻撃シナリオは、マルウエア/偽情報拡散、ネットワーク分断による情報錯綜とし、手段としてノード破壊、不正リンク増設及びその組み合わせとした。これらの攻撃シナリオ及び攻撃手法の組み合わせによる効果は攻撃対象となるネットワーク形状によって異なることを示した。特に基幹ノードの攻撃よりも効率の良い、複数の準基幹ノード攻撃を示し、一般的に考えられるような基幹を狙うことが有効ではない場合があることを示した。

2)の手法として、本研究では Slow Read DoS 攻撃に注目した。この攻撃手法は通常の Three-way hand shake を行なった後で、データの転送量を決定するパラメータ Window のサイズを極端に小さくして、通信速度を意図的に遅くする。接続されたサーバは、通信リソースを占有されてしまう。この手段で大量のコネクションを張られると、サーバは新たな通信要求を受け付けることができず、別のユーザからはサーバダウンしているように見える。一方、サーバ側は通常に運営しているので、攻撃の検知が非常に難しい。注目しているのは、通信を止めているので、ネットワークのトラフィックには全く影響のない点である。この結果、サーバ(ノード)のみ落ちることとなるので、ルーティングが有効に機能しない。本研究の結果、現在知られている対策は 2 人の攻撃者が交互に攻撃する同期型攻撃手法に対して脆弱であり、現時点では有効な対策が見当たらないという結論となった。非常に憂慮すべき結果であり、本研究のテーマ遂行にも大きな影響を与えた。現在継続している研究結果からも、攻撃効果をさらに効率よくする手段は見つかっているものの、防御手段がせいぜい通信環境を悪くする、サーバの処理能力を上げる程度である。また Web サーバ限定であることから、SDN のようなノードに対する有効性の評価が必要である。

(4)ユーザの権利確保とプロトコルの提案

ここでは、特に SNS で生じているプライバシー問題に取り組んだ。本研究の大きな成果は受動プライバシーを定義付け、これを達成するのに必要な安全性要件を導出したことである。これを実現するには、秘密分散手法と属性暗号化技術が必要となる。また、データマイニングを用いた個人情報の暴露の問題にも取り組み、上記と合わせたプロトコルの提案を行なった。ただし、本手法では信頼できる第三者(Trusted Third party, TTP)が必要となる。プライバシーの議論において、プライバシーが損なわれて初めて達成できていなかったことがわかる(逆に言えばプライバシーが守られていることを事前に確認できる手段がない)という典型的な喪失概念であるため、TTP の設置が適切であるか否かの議論が残った。

一方で、大学生/高校生を対象とした SNS 利用状況やプライバシーに関する考え方に関する調査を行なった。マスメディアや教育現場での取り上げ方が大きかったためか、平成 27 年度時点では本研究を開始した時点に比べて、大きな問題とはなっていないことが分かった。所謂、リテラシー教育や SNS を前提とした人付きあいが確立されている傾向にあることが実感できた。また、話題性と必要性の変化が大きいため、研究テーマの選択の難しさも実感した。

当初目的では包括的な研究を行うことであったが、上述のように各要素に分散し、それぞれで結果を出す形となった。また、技術の爆発的普及及び、それに付随するユーザの考え方の変遷があり、当初考えていたプライバシー問題は、その時点ではホットトピックスであったが現在では、あまり注目されていない。研究を通じて技術進展とユーザ意識の関係に注目するきっかけとなった。さらに、実際には導入は不可能であったが、当初の実験ネットワークは小型 PC を想定していた。これはフットプリントで B5 サイズ未満のものである。しかしラズベリーパイの登場により、

このような実機実験環境の構築は劇的に変化した。値段とスペースの関係が、科研費期間内でこれほどまでに大きく変化するのは想定外のことで、今後の応募において検討しておきたい。

研究内容に関しては、それぞれ上記にあげた4つの内容で、発展的なテーマの発見に成功した。また、それぞれで研究成果を挙げる体制も整い、今後の研究進展はかなり期待ができる。具体的に、期間終了後の平成29年6月現在で、計4件の国際学会への投稿、計2件の論文誌投稿の成果となっている。

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12件）

[1]Hiroaki Mizuno, Keisuke Iwai, Hidema Tanaka, Takakazu Kurokawa, Information theoretical analysis of side-channel attack, Information System Security, Springer LNCS.8303, pp.255-269, 査読有(2013)

[2]Junhan Park, Keisuke Iwai, Hidema Tanaka, Takakazu Kurokawa, Analysis of slow read DoS attack and countermeasures on web servers, International Journal of Cyber-Security and Digital Forensics, Vol.4, No.2, pp.339-353, 査読有(2014)

[3]Haruhisa Kosuge, Keisuke Iwai, Hidema Tanaka, Takakazu Kurokawa, Search algorithm of precise integral distinguisher of byte-based block cipher, Information Systems Security, Springer LNCS.9478, pp.303-323,査読有(2015)

[4]Hidema Tanaka, Network Counter-attack Strategy by Topology Map Analysis, Information System Security, Springer LNCS.10063, pp.243-262,査読有, DOI:10.1007/978-3-319-49806-5_13

[5]Haruhisa Kosuge, Hidema Tanaka, Algebraic Degree Estimation for Integral Attack by Randomized Algorithm, Information Security Applications, Springer LNCS.10144, pp.292-304,査読有, DOI:10.1007/978-3-319-56549-1_25

[6]Hidema Tanaka, Security analysis of generalized confidential modulation for quantum communication, International Journal of Computer Networks & Communications, Vol.5, Vol.5, pp.117-129, 査読有(2013)

〔学会発表〕（計27件）

[1]Yusuke Tsuge, Hidema Tanaka, Quantification for Intrusion Detection System using Discrete Fourier Transform, International Conference on Information Science and Security 2016, 予稿集 p.11-16(タイ 2016/12/19-22)査読有

[2]Haruhisa Kosuge, Hidema Tanaka, Keisuke Iwai, Takakazu Kurokawa, Computational security evaluation of light-weight block cipher against integral attack by GPGPU, Cyber Security and Cloud Computing, 予稿集 pp.68-73(ニューヨーク 2015/11/3-5)査読有

[3] Enkhbold Chimedtseren, Keisuke Iwai, Hidema Tanaka, Takakazu Kurokawa, Intrusion detection system using discrete Fourier transform, 7th IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 予稿集 CS3-1(ベトナム 2014/12/14-17)査読有

[4]Sachiko Kanamori, Kanako Kawaguchi, Hidema Tanaka, Study on a Scheme for the Right to Be Forgotten, International Symposium on Information Theory and Its Applications (ISITA 2014), 予稿集 pp.55-59(メルボルン 2014/10/26-29) 査読有

[5]Junhan Park, Keisuke Iwai, Hidema Tanaka, Takakazu Kurokawa, Analysis of slow read DoS attack, International Symposium on Information Theory and Its Applications (ISITA 2014), 予稿集 pp.60-64(メルボルン 2014/10/26-29) 査読有

[6]Hidema Tanaka, Security analysis of generalized confidential modulation, Third International Conference on Computer Science, Engineering & Applications, 予稿集 pp.21-31(デリー 2013/5/24-26) 査読有

６．研究組織

(1)研究代表者

田中秀磨(TANAKA, Hidema)
防衛大学校・電気情報学群・准教授
研究者番号:30328570