別紙様式８

研　究　主　論　文　抄　録

論文題目　統計量を用いたネットワーク攻撃の高精度な検出手法に関する研究
（　Research on the High-precision Detection Method
for Network Anomaly Attacks using Statistics　）

熊本大学大学院自然科学研究科　情報電気電子工学専攻　先端情報通信工学講座
（　主任指導　　末吉　敏則　教授　）

論文提出者　　小島　俊輔
（　by　　Shunsuke Oshima　）

主論文要旨

近年，コンピュータウィルスによる感染被害や各種サーバに対する妨害，サービスの停止を狙ったDoS/DDoS（Denial of Service/Distributed DoS）攻撃などのサイバー攻撃が後を絶たない．DoS/DDoS攻撃，コンピュータウィルスやワーム，攻撃自動化プログラム（通称ボット）に感染したPCのパケットを瞬時に，かつ自動的に発見できれば，サイバー攻撃の被害を最小限に抑えることができる．攻撃検知とは，これら攻撃において生じた通常とは異なるトラヒックの変化をパターンマッチングや統計処理を駆使して発見することである．侵入検知システム（IDS:Intrusion Detection System）は，ネットワークやホストに設置した機器やソフトウェアにおいて，攻撃検知を行い，検知結果を管理者に通知する機能を提供する．現在，多くのIDS製品が市場に出ており，それらの製品の性能を向上させるための攻撃検知手法が日々研究されている．

本研究の目的は，統計的攻撃検出手法において，正確性，すなわち攻撃パケットを攻撃，通常パケットを攻撃でないと正しく判定する性質を向上させた検知手法を提案することである．この正確性を妨げる要因が誤検知であり，誤検知には，攻撃を攻撃と判定できないFalse-Negative，攻撃でないのに攻撃と判定するFalse-Positiveがある．通常，これらはトレードオフの関係にあり，両方を同時に減らす手法を開発することが，攻撃検知の研究分野において最も重要なテーマとなる．本研究では，統計的検知手法の中で，エントロピーとχ^2値を用いた手法に着目した．理由として，これらの統計量の計算は，パターンマッチング手法と比較して高速計算性が非常に高く，近年ますます大容量化するネットワークの通信量に対応できるというメリットがあるためである．

第２章では，これまで発表された統計的な攻撃検知に関する研究についてまとめた．これにより，従来のエントロピー手法では，攻撃多様性と追従性に問題があることを示し，また，従来のχ^2手法では，組織多様性と追従性に問題があることを示した．次に，窓幅やBin（ビン）数などのパラメータに関する基礎資料となるデータを収集するため，従来手法

による実験結果を示している．この実験により，確率変数とすべき特徴量として，送信元IPアドレスや送信先ポート番号が有効であり，また，統計処理すべきパケットの数として，数百から数千が適切であることを示した．

第３章では，攻撃検知や侵入検知，サイバー攻撃などの分野において攻撃の検知性能を評価するために公開されている各種データセットについてまとめた．調査の結果，本研究で用いるデータセットとして，DARPA（Defense Advanced Research Projects Agency:国防高等研究計画局）データセットを選択した．DARPAデータセットは，多くの種類の攻撃を含んでおり，攻撃パケットや通常パケットに匿名化などの加工が施されておらず，さらに，すべての攻撃パケットに付与されたラベルにより攻撃検知の正確性を客観的に評価することができる．

第４章では，エントロピー手法にマハラノビス距離を適用した統計的手法であるEMMM（Entropy-based Multi-dimensional Mahalanobis Method）を提案した．従来手法と比較した結果，EMMMはDDoS攻撃やIPアドレススキャンを高い精度で検知し，正確性に加え攻撃多様性を有することを示した．さらに窓幅を狭くした場合の評価実験，および攻撃パケットの割合を時間とともに変化させた場合の評価実験を行った．その結果，EMMMは即応性と追従性を備えた手法であることを示した．

第５章では，χ^2値をベースにした，複数の特徴量を同時に攻撃に用いることができるCSDM（Chi-square-based Space Division Method）を提案した．提案する手法を用いて攻撃検知の性能を評価した結果，従来手法と比較して，正確性が向上することを示した．また，CSDMの性能を向上させるため，CSDMにおいて補助的に使用する動的Bin手法を提案した．この動的Binは，窓幅やBin幅などのパラメータの設定と，通常パケットの学習という２つの機能を１つに集約する．動的Binを用いたCSDMを評価したことで，提案手法は，組織多様性に加え，追従性を備えた手法であることを示した．

第６章では，第４章および第５章の提案手法の特性を調査した．まず，提案手法における複合攻撃に対する特性を評価した．χ^2値をベースにしたCSDMにおいて，DoSとDDoSを組合せた２重攻撃，および３重攻撃を加えた攻撃検知の評価を行った結果，CSDMはエントロピーベースの手法と比較して，複合攻撃耐性を有することが明らかとなった．次に，提案手法においてパケットの観測から検知までに要する遅延を，待機遅延と計算遅延という２つの遅延に分類して検討した．理論的な計算量の検討と実際の計算時間の計測の結果，処理遅延は，EMMM，CSDMのいずれの提案手法においても，たかだか数秒以下の時間で計算が終了することを示し，高速計算性を有することを示した．

最後に，第７章において本研究を総括し，今後の課題について述べている．