様式３

論　文　内　容　の　要　旨

氏　　名　（　　工藤　隆則　　）	
論文題名	パケットサンプリングを用いた異常トラヒックのオンライン検出に関する研究

論文内容の要旨

第１章では、まずインターネットの異常トラヒックを中心とした本研究の背景について述べた。さらに、ネットワーク内部でトラヒックを計測する際に必要となる主要技術として、パケットサンプリング、フロー集約、スライディングウィンドウ方式によるデータ更新の３点について解説した。

第２章では、高パケットレートフローのオンライン検出におけるパラメータ決定手法について述べた。まず、パケットサンプリングによるトラヒックデータの取得とスライディングウィンドウ方式によるデータ更新を採用した高パケットレートフローのオンライン検出手法について述べた。その後、検出対象である高パケットレートフローの検出確率や検出対象外の低パケットレートフローの誤検出確率、オンライン検出の実行可能性などを考慮したパラメータ決定手法を提案した。実トレースデータを用いた数値実験により提案手法の評価を行った。

第３章では、一定時間以上高いパケットレートが続くような、持続的高パケットレートフローのオンライン検出手法と、そのパラメータ決定手法を提案した。まず、検出対象について述べ、パケットサンプリングとスライディングウィンドウ方式を組み合わせたオンライン検出手法を提案した。具体的には、連続する複数の重複を許したスライディングウィンドウのいずれにおいても、サンプルパケット数が閾値を超えたフローを検出する。このとき検出確率はウィンドウが重複することの影響で計算により求めることが非常に困難となる。その問題を解決する手法と根拠を示し、パラメータ決定手法を提案した。実トレースデータを用いた性能評価実験により、提案手法の有効性を示した。

第４章では、ポートスキャントラヒックのオンライン検出について述べた。まず、ＴＣＰポートスキャンの特徴について触れ、その特徴を利用してＴＣＰポートスキャンを実行しているホストを検出する方法を述べた。なお、この検出手法ではパケットサンプリングとBloomフィルタを利用した。ポートスキャンを実行しているホストを見逃してしまう確率と、ポートスキャンを行っていない正常なホストを誤って検出してしまう確率の両方を保証した上で、使用するメモリ領域や処理コストを最小限に抑えられるようなパラメータの決定手法を提案した。実トレースデータを用いた性能評価の結果は非常に良好で、提案手法の有効性が確認された。

第５章において、本論文の結論を述べた。

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　工藤　隆則　）	
論文審査担当者	（職）　氏　名 主査　教授　滝根　哲哉 副査　教授　馬場口　登 副査　准教授　松田　崇弘 副査　教授　北山　研一 副査　教授　三瓶　政一 副査　教授　井上　恭 副査　教授　鷲尾　隆

論文審査の結果の要旨

グローバル社会を支える基盤インフラとなっている大規模 IP ネットワークのセキュリティを確保し，安定的に運用することは非常に重要である．特に，サイバーテロに代表されるようなネットワークを介した悪意のある活動は社会全体に大きな損害を与える可能性があるため，その発生を早期に検出し，損害の未然防止や拡大阻止を行う技術の確立が急務である．

このような背景の下，本論文はネットワーク管理者の立場から，IP ネットワークで発生する異常トラヒックのオンライン検出を，処理負荷軽減のためにパケットサンプリングを併用して行う手法に関する研究をまとめたものであり，その成果の概要は以下の通りである．

（1）広域ネットワークにおいて，DoS 攻撃などに伴って発生する高パケットレートフローを，ランダムパケットサンプリングとスライディングウインド方式を組み合わせてオンライン検出する手法において，所与の見逃し確率を達成しつつ誤検出率を最小化するシステムパラメータ決定問題が，ウインド内でサンプルされるパケット数を最大化する数理計画問題として定式化可能なことを示している．さらに，定式化された数理計画問題が大域的最適解をもつことを示し，大域的最適解を陽な形で与えている．

（2）広域ネットワークにおいて，持続的な高パケットレートフローをランダムパケットサンプリングとスライディングウインド方式を組み合わせてオンライン検出する手法において，所与の見逃し確率を達成しつつ誤検出率を最小化するシステムパラメータ決定問題を，上記（1）で得られた知見を援用して数理計画問題として定式化している．持続的な高パケットレートフローの検出では，連続するスライディングウインド間での相関を考慮する必要があるため，システムパラメータ決定問題は，上記（1）と比較して，格段に複雑な問題となるが，準最適な閾値フローを導入することで定式化に成功している．

（3）ローカルネットワークの端点において，ポートスキャンを実行するローカルネットワーク内のホストをランダムパケットサンプリングとジャンピングウインド方式を組み合わせてオンライン検出する手法において，所与の見逃し確率ならびに誤検出率を達成しつつサンプリングレートを最小化するシステムパラメータ決定問題を数理計画問題として定式化し，実行可能であるための条件を明らかにしている．

（4）上記三つの検出手法のそれぞれに対して，本論文で与えた手法を用いて具体的にシステムパラメータの値を決定し，実トレースデータに適用することで検証実験を行い，想定通りの異常トラヒック検出性能が発揮されることを確認している．

以上のように，本論文はランダムパケットサンプリングを併用した各種の異常トラヒック検出手法におけるシステ

ムパラメータを，見逃し確率，誤検出確率の双方を考慮して決定する枠組みを与えている．従来の研究において，複雑に絡み合うシステムパラメータの決定手法を議論した論文はほぼ皆無であり，本論文で提案されたシステムパラメータ決定手法は斬新，かつ実用上も極めて有用である．よって本論文は博士論文として価値あるものと認める．