論 文 内 容 の 要 旨

博士論文題目 Protecting IP Telephony against SPIT and SIP Flooding Attacks
「IP テレフォニーを SPIT と SIP フラッド攻撃から保護する手法に関する研究」

氏　　名 Noppawat Chaisamran

The global communication market is rapidly moving toward IP (Internet Protocol) telephony. Similar to other IP-based applications, it is vulnerable to several attacks. Therefore, security concerns become more important for users and service providers. In this dissertation, real-time attack detection systems are proposed to protect the IP telephony against Spam over Internet Telephony (SPIT) and Session Initiation Protocol (SIP) flooding attacks. It consists of three main contributions.

First, a trust-based SPIT detection based on calling behavior and human relationships is introduced to classify calls. A call duration and its direction as well as a calling ratio of each user are used to calculate a trust value. This trust value is automatically adjustable according to the call characteristics in order to keep track of a current user's behavior and avoid bias in trust value assignment.

Second, an anomaly-based SIP flooding attack detection system is proposed to detect a significant deviation in SIP traffic. Three statistical algorithms are used to analyze incoming traffic to a server: an application of Tanimoto Distance, an adaptive threshold, and a Momentum Oscillation Indicator. Due to a stateless and low computational cost of these algorithms, the proposed system can classify traffic in nearly real-time that is suitable for an IP telephony system.

Lastly, false positive alarms of the flooding attack detection are reduced by using a trust filtering. A reliable trust value is calculated through the call activities and the human behavior of each user. The trust value of suspicious callers will be checked before raising any alarm.

氏　名	Noppawat Chaisamran

（論文審査結果の要旨）

本博士論文では、IP テレフォニーを SPIT と SIP フラッド攻撃という本質的に避けられない２つの重要な問題から保護する手法の提案を行っている。第一に，SPIT は呼を着信するユーザを直接的にサービス妨害するため，e-mail スパムよりも深刻な問題となり得る．本博士論文では，発呼者と着呼者の信頼関係を，これまでの呼の方向とその長さによって定義することで，SPIT を発信しているユーザを高い精度で区別することに成功している．この信頼関係は，各契約者の発信履歴のみから自動的に生成，調整される．直接通話したとこのない発信者に対しては，データ融合技術とソーシャルネットワークからの知見を用いることで信頼関係の推測を行っている．実際の電話回線の通信統計や，SNS データに基づいた実験から，高精度で SPIT 発信者の識別が可能であることを確認している．この手法の優れている点は，加入者や既設の網に対する変更を必要とせず，実時間で SPIT を検出できる点である．技術的，社会的にも意義のある提案であると考えることができる．

第二に，IP テレフォニーは，従来の公衆電話回線に比較して，数々のサービス妨害攻撃に曝されることになる．現在の IP テレフォニーが基盤としている SIP では，攻撃者が SIP サーバに対して大量の SIP メッセージを送付することで，容易にサービス妨害攻撃を実行できる．本博士論文での提案では，統計情報と多変量モデルを用いて攻撃を検出する．そのため，攻撃者がこのシステムを無力化するのは困難である．さらに誤検出を低減するため，信頼関係を用いて攻撃検出手法を強化した．シミュレーション結果から，提案システムが様々な種類のフラッディング攻撃に対しての有効性を確認している．

以上により、本博士論文は研究内容について新規性並びに有効性があることが認められ、博士（工学）の学位を授与するにあたって十分な内容であると認められる。

氏　名	Noppawat Chaisamran

（最終試験結果の要旨）

本博士論文は、IP テレフォニーを SPIT と SIP フラッド攻撃から保護する手法に関する研究である。IP テレフォニーにおける VoIP スパムと，IP テレフォニーの基盤となる SIP システムに対するフラッディング攻撃に対する防御手法をまとめたものである．本論文審査の中で、審査委員から数点の改善事項が提示され、最終的に全ての項目について改善が見られた。以下に最終審査の結果概要を示す。

（1） SPIT 発信者の比率が最低 1%までの評価しか行われていないが，現実的な比率かという指摘に対して，さらに低い比率でのシミュレーション結果を追加し，SPIT 発信者の比率がより低い場合でも検出精度を高いレベルに維持できることを示した．

（2） SPIT 検出と SIP フラッド攻撃検出にかかる計算オーバヘッドも評価すべきという指摘に対して，データをもとに評価し，現実的な想定環境内では提案システムが膨大な資源を消費することがなく，前提とする SIP システムをサポートできることを確認した．

（3） SPIT 検出システムの将来的な実環境への導入に関して，実際の現場では想定できないトラブルが起こりえる．これらを踏まえて導入へシナリオを考えるべきであるという指摘に対して議論を追加し，システム異常時に運用者がどのように対処すべきかの議論を行った．

指摘事項に対して十分な改善が見られ、本博士論文は博士（工学）の学位を授与するのに充分な内容であり、独立した研究者として研究開発を継続するに充分な素養を備えていると判断できる。

なお、2014 年 2 月 21 日、全審査委員により、学位申請者に対して論文内容及び関連事項についての試問を行い、充分な知識を持つ物と認められたので合格と判定した。