京都工芸繊維大学

氏　　名	きむら さとし **木村　知史**
学位(専攻分野)	博　士（工学）
学位記番号	博甲第 996 号
学位授与の日付	令和 3 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
研究科・専攻	工芸科学研究科　設計工学専攻
学位論文題目	Practical Operating Method for Intrusion Detection System Using Machine Learning and Visualization （機械学習及び視覚化を用いた実用的な IDS の運用手法）
審査委員	(主査)教授　稲葉宏幸 教授　梅原大祐 教授　桝田秀夫

論文内容の要旨

近年、あらゆる分野においてインターネットは重要な役割を果たすようになってきており、それに伴ってネットワークセキュリティの重要性が強く認識されるようになっている。侵入検知システム(IDS)は、ネットワークにおける様々なサイバー攻撃やそれに準ずる行為を検知する装置であり、ネットワークセキュリティを実現する上で重要な役割を果たしている。しかし、一般に IDS は大量の検知アラートを出力するため、IDS の効率的な運用は必ずしも容易ではない。そこで、本論文では、機械学習およびデータの視覚化手法を用いることにより、より現実的な IDS の運用手法を提案している。

本論文第 3 章ではまず、管理者が日常的に観測される検知アラートとそうでないアラートを明確に区別できる検知アラートの視覚化システムを提案している。このシステムでは、表示スケールを検知結果に応じて自動的に変更することで、膨大な IP アドレス空間を同時に表示することを可能にしている。また、過去に観測された検知アラート数から動的にしきい値を算出することで、非日常的な検知アラートの強調表示を可能にしている。

次に、本論文第 4 章では、IDS において一般的に観測される検知アラートが、(1)定常的なもの、(2)周期的なもの、(3)突発的な大量検知、の 3 種類に大きく分類できることを実データから明らかにしている。そして、この性質を用いることにより、日常的に観測される検知アラートの変化を、指数平滑法の一種である Holt-Winters 法を用いて予測する手法を提案し、実データを用いてその予測精度を示している。

また、本論文第 5 章では、インターネットにおける最も重要なサービスの一つである Domain Name System(DNS)に対するサイバー攻撃に着目し、DNS パケット数の時間変化を、深層機械学習の一種である LSTM を用いて学習し、高い精度で DNS パケット数の変化を予測できることを示している。これにより、DNS プロトコルを悪用する DNSamp 攻撃等を早期に検知することが可能となる。

本論文で提案された手法により、IDS の管理者は、大量の検知データログを手動で解析することなく、ネットワークの状態を把握することができ、より効率的なネットワーク管理が可能にな

る。

論文審査の結果の要旨

本論文の成果は、IDS の現実的な運用を実現するために、検知結果の視覚化手法と、シグネチャ毎の検知数の傾向を学習し将来の検知数を予測可能とする手法を与えるものであり、IDS の運用管理者の業務の効率化に大きく貢献できると考えられる。

検知結果の視覚化手法では、IDS が出力する膨大な検知結果を、画面を切り替えることなく一覧できる機能を提案している。これは、IP アドレスを表現するスケールを動的に決定することで実現しており興味深い手法である。また、過去の検知数に基づいてしきい値を自動的に決定し、管理者が注目すべき検知アラートを強調表示することも可能としている。

IDS が検知するアラートの中には、日常的に観測されるものも多くあり、個々のアラートには大きな危険はないものの、アラート数が急激に増加するような場合には何らかの対応が必要になることも多い。本論文で提案されている手法は、定常的に観測される検知アラートのみならず、周期的な変動をもつ検知アラートについても、その検知数の変化を学習できる手法であり、将来の検知数の変化を適切に予測可能である。本論文では、検知数を逐次的に予測する手法の他に、予測精度がやや劣るものの一定期間の検知数をまとめて予測する手法も提案しており、管理者が多様なセキュリティ対策を行うことを可能にしている。

さらに、本論文第 5 章では、DNS パケット数の時間変化を LSTM を用いて学習し、将来の DNS パケット数を高精度に予測する手法を提案している。これにより、DNSamp 攻撃等の早期検知が可能となると考えられる。また、LSTM の予測値に基づいてアノマリー検知を行う場合に、異常性を判定するしきい値を動的に決定する手法を示しており、管理者に有用なツールになりうると判断できる。本提案手法は、他のプロトコルにも容易に拡張できると考えられ、今後のさらなる進展が期待できる。

本論文は、申請者を筆頭著者とする査読を経た以下に示す 3 編の論文を基礎としている。

1. Satoshi Kimura, Hiroyuki Inaba：An IDS Visualization System for Anomalous Warning Events, International Journal of Networked and Distributed Computing (IJNDC), Vol.2, No.1, pp.45-53, 2014.
2. Satoshi Kimura, Hiroyuki Inaba：IDS Operation Management Method Using Holt-Winters Method, 2017 IEEE 6th Global Conference on Consumer Electronics(GCCE), pp.425-429, 2017.
3. KIMURA Satoshi, INABA Hiroyuki：Proposal of Anomaly Detection for DNS Attacks Based on Packets Prediction Using LSTM, 2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.90-95, 2020.