論 文 内 容 の 要 旨

博士論文題目 Unsupervised Anomaly Detection in Massive Traffic Using S-transform and Rényi Divergence (S 変換 と Rényi ダイバージェンスを用いた大規模トラフィックにおける教師なし異常検知)

氏　　名 Sirikarn Pukkawanna

The detection of network anomalies is an indispensable component of overall security architecture. As sophisticated attacks grow exponentially, preserving security with signature-based Network Intrusion Detection Systems (NIDS) may not sufficient because they cannot detect unknown and new attacks. In this dissertation, we propose two novel network anomaly detection methods: S-transform-based and Rényi divergence-based methods.

The S-transform-based anomaly detection method uses S-transform to convert a traffic signal (e.g., packet rate) to a time-frequency domain and the method then detects unusual time-frequency behavior caused by anomalies in the time-frequency domain. The results indicated that our improved method provided higher accuracy and lower false positive rates.

The Rényi divergence-based anomaly detection method can detect anomalies based on the Rényi divergence of the port pair distributions. The results indicated that our feature completely outperformed the four widely-used features, namely the distributions of source IP, destination IP, source port, and destination port in terms of both accuracy and false positive rates. Lastly, we compared the performance of our method with a Kullback-Leibler (KL) divergence-based anomaly detection method. The results indicated that our method could detect anomalies with 96% accuracy and was more effective than the KL divergence-based method.

氏　名	Sirikarn Pukkawanna

（論文審査結果の要旨）

本博士論文では，ネットワークセキュリティ上不可欠な異常検知に関して，２つの主要な提案を行っている．

一つ目は S 変換を用いた教師なし異常検知手法と，スケッチを用いた改良である．時間—周波数空間の変化も考慮する事により，従来の時系列変化に基づいた異常検知手法ではとらえられない周波数方向に変化する異常も検知可能となった．実際のトラフィックデータと生成したトラフィックデータに対して本手法を適用した結果，高い精度で異常検知に成功し，同時に擬陽性を低く抑える事に成功している．

二つ目は入力データとしてポートの対の分散のみを用いて異常検知を行う手法である．ポート対の Rényi divergence に基づいた，シグネチャやラベル付き教師データを用いない異常検知手法を開発した．従来使われている IP アドレスの対，ポートの対を用いるよりも処理データ量を削減し，Kullback-Leibler divergence に基づいた手法やより多くの指標を用いた手法よりも高い精度と低い擬陽性を達成できる事を，実トラフィックを用いた実験により確認した．

提案されている２つの手法は実用に供する事を目的として時間・空間計算量ともに低く抑えられており，かつ実時間での異常検知も可能である．

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。

（Ａ４　１枚　１，２００字程度）