IoT 環境のための軽量な侵入検知と高速な攻撃防御に関する研究

氏　　名　桂 祐成

研 究 室 名　情報基盤システム学研究室

主指導教員名（論文博士の場合は推薦教員名）　藤川 和利 教授

内 容 梗 概（1ページ目に収めること）

IoT 機器は計算リソースに制約があるため, 計算リソースを必要とする複雑なセキュリティ対策を実装することが困難である．この制約により，IoT 機器の脆弱性を狙った攻撃が数多く観測されている．このような攻撃から IoT 機器を守るため，IDS と SDN システムを組み合わせた手法が提案されている．しかし，既存手法では，IDS が攻撃を検知し，ログファイルにアラートを出力した後，ログ監視ツールが REST API 介して SDN システムに攻撃の遮断設定を行うため，オーバーヘッドが発生していた．本研究では，Syslog と OpenFlow プロトコルの Packet-In メッセージを併用することで，攻撃の検知から遮断設定までのオーバーヘッドを削減した．また，IoT 環境における侵入検知システムでは，既存研究の多くが侵入検知単位としてパケット単位およびフロー単位の侵入検知手法を採用している．そのため，パケットやフローの組み合わせパターンが多く表れる一部の攻撃では，検知処理時に高い計算リソースを要するという課題があった．この課題を解決するため，本研究では，従来のパケット単位およびフロー単位での侵入検知をホスト単位に変更し, IoT 機器の通信挙動をエントロピーで表現する手法を提案した．この手法により，7 つの特徴量と軽量な機械学習アルゴリズムを用いた場合においても，高い検知精度を維持しつつ，検知処理時の処理時間とメモリ使用量の削減を実現した．この研究では，様々な IoT 機器のパケットキャプチャデータを含むデータセットを使用し，1 秒間隔から 30 秒間隔までの侵入検知精度を評価することで，提案手法の有効性を示した．これらの手法を組み合わせることで, IoT 環境における侵入検知の処理時間とメモリ使用量を削減し，軽量な侵入検知と高速な攻撃防御の実現を可能にした．