Computer Security Symposium 2018
22 - 25 October 2018

IoT機器に特化したアノマリ型侵入検知システムの提案

瀧本 達也[1]　稲葉 宏幸[2]

概要：近年，インターネットの発展に伴い，生活のあらゆる場面で多くの IoT 機器が利用されている．一方で，IoT 機器を狙った様々なサイバー攻撃が報告されており，この対策として侵入検知システム (IDS) がしばしば用いられている．IDS はシグネチャ型とアノマリ型の 2 種類に大別できる．前者は未知の攻撃を検知することはできないが，後者は未知の攻撃を検知することが可能である．その反面，正常な状態を定義することが難しいという問題がある．そこで本稿では，IoT 機器の場合には一般的な PC 等とは異なり，その通信内容は限られた種類のパケットからなることが多い点を利用して，その通信ログから正常動作のモデルを生成し，これを利用することで，IoT 機器に特化したアノマリ型 IDS を提案する．

キーワード：IDS，IoT，主成分分析，異常検知，LOF

Proposal of Anomaly Intrusion Detection System Specialized for IoT Devices

Tatsuya Takimoto[1]　Hiroyuki Inaba[2]

Abstract: In the recent years, with the development of the Internet, many IoT devices are used in every aspect of life. On the other hand, various cyber attacks targeting IoT devices have been reported. Intrusion Detection System (IDS) is often used as a countermeasure against this. IDS can be generally divided into two types, signature type and anomaly type. While the former can not detect unknown attacks, the latter can detect such attacks. On the other hand, there exists a problem that it is difficult for anomaly type to define a normal state. However, in the case of IoT devices, the communication log is often composed of limited types of packets unlike general PC. We generate a model of normal state of IoT communication, and we propose an anomaly IDS specialized for IoT devices.

Keywords: IDS，IoT，principal component analysis，anomaly detection，LOF

1. はじめに

近年，インターネットの発展に伴って，一般家庭や学校，企業など生活のあらゆる場面で多くの IoT 機器が利用されている．

一方で，IoT 機器に対するセキュリティ対策が不十分なまま普及が進んだため，IoT 機器を狙った様々なサイバー攻撃が報告されている．例えば，2016 年に観測されたマルウェア Mirai は，大量の IoT 機器に感染し，それらを用いたサービス妨害攻撃により，多くのネットワークサービスが被害を受けた．[2]

このようなサイバー攻撃への対策の一つとして，攻撃を自動で検知するための侵入検知システム (IDS) がある．今日の多くの IDS では検知率の観点からシグネチャ型 IDS が採用されているが，Mirai のように短期間で多様に変化するマルウェアに対して，検知を行うことは難しい．一方で，アノマリ型 IDS は，このようなマルウェアに対して有効な手法ではあるが，多種多様な動作をするインターネット接続機器に対して正常動作のモデルを構築する必要があるため，その検知精度を高めることは難しく，また多大な

[1] 京都工芸繊維大学大学院情報工学専攻
Graduate School of Information Sciences, Kyoto Institute of Technology
[2] 京都工芸繊維大学 情報工学・人間科学系
Faculty of Information and Human Sciences, Kyoto Institute of Technology

コストがかかってしまうデメリットがある．

しかし，一般的な PC やルーター機器などではなく，例えばネットワークカメラのような IoT 機器の場合であれば，通常は録画データを特定の相手に送信する等の限られた動作をしており，それ以外の振る舞いは行っていない．このように，限定的な振る舞いをする機器は，その通信ログも一般的な PC やルーター機器とは異なり，限られた種類のパケットのみからなることが予想される．したがって，IoT 機器の正常な動作を一定の期間観測することで，比較的容易に正常動作のモデルの構築が可能であると想定される．

そこで本稿では，上述した仮定に基づき，IoT 機器の通信ログから正常動作のモデルを生成することを考える．さらに，このモデルを IDS に適用し，IoT 機器に特化したアノマリ型 IDS を提案する．

2. 関連研究

本節では，IoT 機器のセキュリティ問題に対する研究及びネットワークトラフィックから異常検出を行なっている研究を紹介する．

IoT 機器のセキュリティに対する研究として，文献 [3] では一般消費者の家庭環境を模擬した 16 種類のネットワーク接続可能な機器からなるテストベッドを構築し，疑似的な攻撃をテストベッド内で試行することで機器への影響を検証する実験を行なっている．テストベッド内の実機に IoT マルウェアを感染させ，その他の IoT 機器に向けて DoS 攻撃を行い，その攻撃耐性について検証した結果，半数以上の IoT 機器が動作不能になることが確認された．

また，文献 [4] では，IoT 機器の Telnet インターフェースに対し多数の攻撃が行われている点に注目し，Telnet ログインの際に得られる ID/パスワード情報とログイン後に使用されるシェルコマンド系列を分析することで，攻撃ホストの感染マルウェアの推定を行っている．さらに，攻撃に用いられる ID/パスワードの増加から攻撃対象となる IoT 機器の増加を確認している．

このように IoT 機器のセキュリティに関しては，未だに十分な対策がされておらず，今後それらを利用した大規模なサイバー攻撃が予想され得る．

本研究と同様にネットワークトラフィックから異常検出を行なっている研究として，文献 [5] ではネットワークトラフィックから特徴ベクトルを抽出し，それらをクラスタリングすることで異常検出を行なっている．具体的には，トラフィックデータを複数の単位時間にわけ，各区間から 61 種類の特徴量を抽出する．その後，得られた特徴ベクトルを Mean-Shift 法を用いてクラスタリングし，異常なトラフィックデータを検出する方法を提案している．

図 1 提案手法の概要

3. 提案手法

本手法の概要を図 1 に示す．本手法は，学習部分と異常検出の部分に大別することができる．まず学習部分では，IoT 機器の正常なトラフィックデータを収集し，それを一定時間ごとのウィンドウに区切る．そのウィンドウ内で，パケットのヘッダ部に含まれる情報を特徴量として抽出し，各ウィンドウごとの特徴ベクトルを生成する．これらを主成分分析を用いて次元圧縮し，それらを特徴空間にプロットする．これは IoT 機器の正常動作モデルを表していると考えられる．次に異常検出の部分では，学習時に用いたトラフィックデータとは別の未知トラフィックデータから同様にして特徴ベクトルを生成し，それを逐一正常動作モデルにプロットする．そして，異常検知手法を用いてそれが正常な通信か否かを判別する．

3.1 通信ログからの特徴量抽出

本研究では，パケットのヘッダ部の情報を特徴量として抽出する．従来，このような手法を用いる場合，以下のような方式が取られている．

(1) パケット単体のヘッダ部から特徴量を抽出する
(2) トラフィックデータを一定時間のウィンドウに区切り，その中で特徴量を抽出する
(3) トラフィックデータをセッションと呼ばれるひとまとまりの通信に区切り，その中で特徴量を抽出する

(1) の方式は基本的な方式であるが，パケット単体から得られる攻撃に関する情報は限定的であり攻撃の検知は難しいという問題がある．(3) では，TCP のように通信相手とセッションを張る通信の特徴を捉えることができるが，UDP を用いた通信を行う IoT 機器には適用することが難しい．したがって，(2) の方式を採用することで，攻撃の一連の流れを含めた特徴を抽出する．ウィンドウ内で抽出する主な特徴量を表 1 に示す．特徴量には，IoT 機器に特化したアノマリ型 IDS を実現するため，一般的にパケットのヘッダ情報を用いた異常検知に使用されるパケットサイズや到着間隔，TCP，UDP パケットの割合などの統計情報

を含めるほか，そのIoT機器特有のポートに対するパケット数や正常動作ログ収集時に得られた送信元IPアドレスのパケット数など合計1127個の特徴量を選択する．

表 1 主な特徴量

パケットサイズ平均
パケットサイズ分散
総パケットサイズ
総パケット数
パケット到着間隔平均
パケット到着間隔分散
telnet，sshなどのwell-knownポートにおける送信元パケット数
telnet，sshなどのwell-knownポートにおける宛先パケット数
TCPパケットの割合
UDPパケットの割合
送信元IPアドレス毎のパケット数

3.2 異常検出

各ウィンドウから構成される特徴ベクトルが類似している場合，特徴空間におけるそれらの特徴ベクトル間の距離は小さくなる．逆に，特徴ベクトルが大きく異なる場合，それらの特徴ベクトル間の距離も大きくなると考えられる．したがって，未知の通信ログから得られた特徴ベクトルと正常な通信ログから得られた特徴ベクトルとの距離が小さければ，それは正常な通信ログである可能性が高い．逆に，距離が大きければ異常な通信ログの可能性が高いと考えられる．そこで，本研究では外れ値による異常検知手法を用いる．外れ値による検知手法には距離に基づくものの他，密度に基づくものなどがある．前者は，k-NN法やクラスタリングを用いた手法があるが，これらは疎密な分布を持つデータに対しては正しく検知することは難しい．逆に，後者は疎密な分布を持つデータに対しても検知精度が優れている．異常な通信から得られる特徴ベクトルはその近傍の局所密度が低くなるため，本稿では密度に基づく外れ値検知手法であるLocal Outlier Factor(LOF)法を用いる．[6] この異常検知手法は，ある特徴点の局所的な密度を計算することでその特徴点が異常かどうかを識別する．

4. 検証実験

4.1 事前実験

本節では，IoT機器の場合には一般的なPC等とは異なり，その通信内容は限られた種類のパケットからなることが多いという仮説を確認するための実験を行う．実際にネットワークカメラ及びPCの通信ログから特徴量を取り出し，それらの特徴を可視化することでこれを確認する．今回はネットワークカメラとしてKEIAN社のC7823WIPを用いた．[7] また，PCのOSはWindows10 Proである．

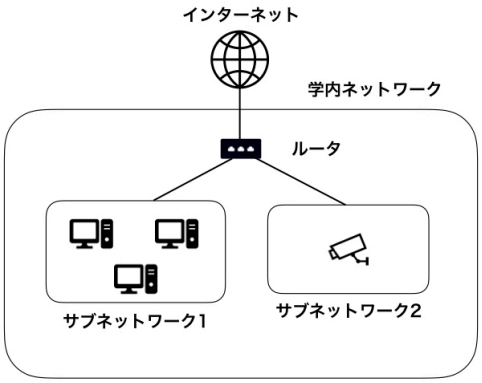

図 2 実験環境

具体的には以下の手順で検証を行う．

(1) PCについては，メールの送受信やネットサーフィンなどの一般的な操作をしている利用時と特に操作をしていない待機時の2種類のログを収集する．ネットワークカメラについても同様に，外部から監視などを行なっている利用時と待機時の2種類のログを収集する．
(2) それぞれを同じウィンドウサイズで区切り，特徴量を抽出する．
(3) 全ての通信ログから得られた特徴ベクトルを主成分分析を用いて，同一の特徴空間上にプロットし可視化する．

4.1.1 実験条件

本実験では，本学学内ネットワークに設置したPC及びネットワークカメラを用いて通信ログの収集を行なった．実験環境の概要を図2に示す．PCの利用時及び待機時の通信ログとネットワークカメラの利用時及び待機時の通信ログをそれぞれ約1時間程度収集し，それらを60秒のウィンドウに区切った．特徴量としては，3.1で説明した特徴量を用いた．さらに，主成分分析を用いて特徴ベクトルを3次元まで圧縮し，特徴点がどのように分布するのかを確認する．

4.1.2 結果

それぞれの通信の特徴点を同一の特徴空間上にプロットしたものを図3に示す．また，この3次元空間の中から特に特徴が見て取れた第1主成分－第3主成分平面を図4に示す．これらから，PCの特徴点はネットワークカメラの特徴点に比べて散在していることがわかる．これは，PCが操作されている際に様々なプロトコルを用いた通信を行なっているためと考えられる．また，ネットワークカメラの2種類のデータはほぼ同じ位置に密集しており，第1主成分及び第3主成分に関して類似した特徴を持つと考えられる．全体として，ネットワークカメラの通信ログは特徴点がある主成分軸に対して密集していることから，ある程度類似したパケットで構成されていると考えられ，PCの通信ログは特徴点が散在していることから，特徴の異なる

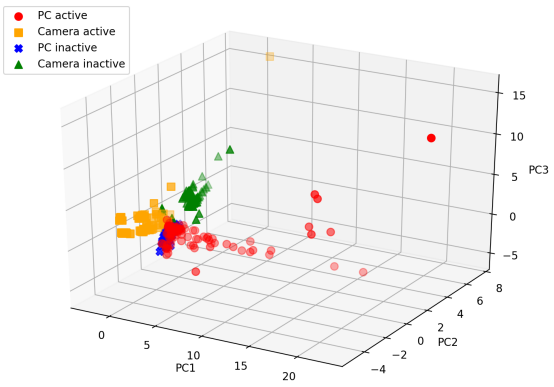

図 3 特徴空間

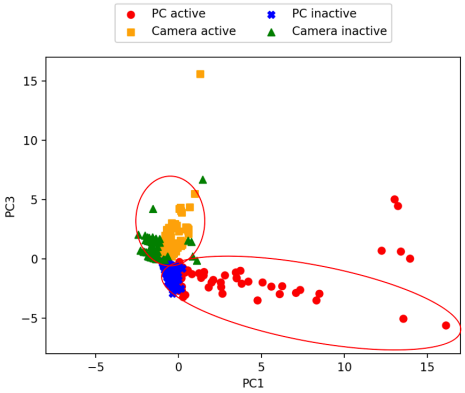

図 4 第 1 主成分－第 3 主成分平面図

様々なパケットから構築されているということが確認できた．

4.2 模擬攻撃に対する検知実験とその評価

事前実験の結果より，IoT 機器の通信ログは限られた種類のパケットから構成されることが多いと考えられるため，本節では提案手法が実際に異常な通信を検知できるのかを確認する実験を行う．具体的には，ネットワークカメラに対して，著者自身がその脆弱性をついた攻撃を模擬する．その模擬攻撃を含んだ通信ログを収集し，提案手法を適用することで検知精度などの評価を行う．

実験に使用したネットワークカメラには，アカウント名及びパスワードを攻撃者に知られてしまうと，FTP の設定用 CGI を悪用することで，telnet によって侵入することができる脆弱性が存在する．一般的な利用者はこのような機器のアカウント名，パスワードをデフォルトのまま放置してしまうことが多いため，攻撃者は容易に侵入することが可能であり，Mirai のようなマルウェアに感染し，ボット化してしまうなどの被害が想定される．実験ではこのような攻撃を模擬する．その手順を以下に示す．

(1) 攻撃者には IP アドレスなどが事前に分かっているものとし，FTP の設定用 CGI を悪用し，telnetd を起動させる
(2) telnet により侵入した後，任意のコマンドを実行する
(3) Mirai による攻撃を模擬するため，スクリプトファイルなどをサーバからダウンロードさせる

このような操作を模擬攻撃として，通信ログに含める．なお，模擬攻撃は学外のネットワークから行なっている．これを提案手法によって異常として識別できるかを評価する．

4.2.1 実験条件

本学学内ネットワーク (ファイアウォールによる制限なし) にネットワークカメラを設置することで通信ログを収集した．正常なトラフィックデータとして，2018 年 7 月 9 日から 2018 年 7 月 10 日に収集した約 24 時間のデータを用いた．これを 60 秒のウィンドウに区切り，そのウィンドウ内で特徴量を抽出することで正常動作のモデルとした．これとは別に正常なトラフィックデータ及び模擬攻撃を含めた異常なトラフィックデータをそれぞれ約 3 時間分用意した．これらも先程と同様にして特徴量を抽出し，各ウィンドウの特徴ベクトルを生成した．最終的にこれらを正常動作のモデルに逐一プロットし，主成分分析を用いて次元圧縮を行う．この時，圧縮後の次元数 n を 5，10，100，500，1000 と変化させて実験を行なった．この後，Local Outlier Factor 法を用いて検知実験を行なった．なお，LOF 法のパラメータである距離を求める近傍点の個数 k も 5，10，100，1000，2000，2900 として実験を行なった．

4.2.2 実験結果及び考察

次元圧縮後の次元数 n 及び近傍点の個数 k ごとの検知率を表 2 に示す．

表 2 検知率 [%]

$n \setminus k$	5	10	100	1000	2000	2900
5	77.5	88.5	57.0	89.5	89.5	90.5
10	41.0	54.0	33.5	41.5	46.5	47.0
100	4.5	6.0	7.5	30.5	38.0	39.5
500	0.0	0.0	9.0	35.5	43.5	44.0
1000	0.0	0.0	10.5	39.0	44.0	45.5

次元圧縮後の次元数 n について，n が小さい方が検知率が高いことがわかった．主成分分析を用いた次元圧縮では分散の小さい特徴量，つまりその特徴量の持つ情報量が少ないものは考慮されなくなる．したがって，攻撃に関する情報を多く持つ特徴量を限定して用いることで，異常なトラフィックデータが検知しやすくなるのではないかと考えられる．また，距離を求める近傍点の個数 k については，値が小さい場合と十分大きい場合に検知率が高くなることがわかった．k が小さい時は，少数の近傍点との距離しか求めていないため，異常なトラフィックデータの特徴点が他の特徴点と十分に離れている場合には正しく異常検知できたと考えられる．また，k が大きい場合は，ほぼ全ての

特徴点との距離を求めているため，データ全体の分布が十分考慮されており，高い検知率が得られたと考える．しかし，k を大きくしていくと距離を求めるデータ点の数が増加してしまい，計算に多くの時間がかかるため，検知率と計算時間のトレードオフになると考えられる．

表 2 から，n 及び k を適切に設定することにより，模擬攻撃に対して 9 割程度の確率で検知できることが確認できた．

5. まとめ

本稿では，IoT 機器の通信パケットのヘッダ情報から正常動作のモデルを生成することで，IoT 機器に特化したアノマリ型 IDS を提案した．まず，実際に学内に IoT 機器を設置し，IoT 機器の通信ログが一般的な PC に比べ限られたパケットから構成されることを確かめるための実験を行なった．その後，IoT 機器に対して著者自身が Mirai に感染させることを想定した模擬攻撃を行うことで，提案するアノマリ型検知手法の性能を評価するための実験を行なった．

今後の課題として，本研究では IoT 機器としてネットワークカメラを用いて実験を行なったが，別の IoT 機器に対しても通信ログが限られた種類のパケットから構成されているかを確かめる必要がある．また，今回は模擬攻撃として限定されたもののみを用いて実験を行なったため，他の攻撃に対する検知精度も検証していく必要がある．

謝辞 本研究にあたり貴重な助言を多数頂きました，本学博士後期課程設計工学専攻木村知史様に厚く御礼を申し上げます．

参考文献

[1] 宮田 健，IoT デバイスを狙うマルウェア「Mirai」とは何か，入手先 ⟨http://techfactory.itmedia.co.jp/tf/articles/1704/13/news010.html⟩，(参照 2018-8-17).

[2] B.Krebs, Krebs On Security Hit With Record DDoS, 入手先 ⟨https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/⟩ (参照 2018-8-17).

[3] 楊 志勇，熊 佳，鉄 穎，田宮 和樹，西田 慎，楊 笛，藤田 彬，吉岡 克成，松本 勉,“ホームネットワークテストベッドによるサイバー攻撃の観測と検証,” コンピュータセキュリティシンポジウム 2017 論文集，vol.1C4，no.2，pp.196-203，2017.

[4] 中山 颯，鉄 穎，楊 笛，田宮 和樹，吉岡 克成，松本 勉,“IoT 機器への Telnet を用いたサイバー攻撃の分析,” コンピュータセキュリティシンポジウム 2016 CSS2016/10，pp870-877.

[5] 谷澤 俊樹，青木 茂樹，宮本 貴朗,“パケットのヘッダ情報に注目したアノ マリ型 IDS とシグネチャ型 IDS を組み合わせた未知の異常検出,” コンピュータセキュリティシンポジウム 2017 論文集，vol.3B4，no.1，pp.1397-1403，Oct. 2017.

[6] Markus M.Breunig, Hans-Peter Kriegel, Raymond T. Ng, Jörg Sander, ’LOF: Identifying Density-Based Local Outliers’, 入手先 ⟨http://www.dbs.ifi.lmu.de/Publikationen/Papers/LOF.pdf⟩ (参照 2018-8-19)

[7] KEIAN 社，ネットワークカメラ C7823WIP，入手先 ⟨https://www.keian.co.jp/products/c7823wip/⟩ (参照 2018-8-19)