L-009

クラスタリングによる外れ値検出に基づくネットワークの異常検知

Network Anomaly Detection Based on Outlier Detection by Clustering

西田 達輝 * 青木 茂樹 * 宮本 貴朗 *
Tatsuki Nishida Shigeki Aoki Takao Miyamoto

1 はじめに

近年，インターネットの普及に伴いサイバー攻撃の多用化と増加が深刻な問題になっている．そのため，サイバー攻撃を検出するための侵入検知システム (IDS：Intrusion Detection System) の研究が盛んにおこなわれている．IDS はアノマリ型とシグネチャ型の 2 種類に大別することができる．シグネチャ型はあらかじめ異常な通信をパターンファイルに保存しておき，パターンファイルに基づいて異常を検知する方式である．アノマリ型は正常な通信パターンのみを学習し，学習した通信パターンから外れた通信を異常として検出する方式である．代表的なアノマリ型 IDS としては文献 [1][2] が挙げられる．

文献 [1] では単位時間ごとに特徴量を抽出しクラスタリングを行うことによって正常状態を定義し，観測データと正常クラスタとの距離によって異常を検出する手法を提案している．この手法では単位時間ごとに特徴を抽出して異常検出を行っているため，処理コストを小さくできるが攻撃元が特定できないという欠点がある．文献 [2] ではセッション単位で特徴量を抽出して DBSCAN によってクラスタリングし，セッション単位のクラスタ遷移をスコアリングすることにより攻撃を検知している．この手法のように，セッション単位で異常検出を行うと攻撃元の特定は容易になるが，処理コストが大きくなるという問題がある．

そこで，本研究では単位時間ごとに送信元 IP アドレスのサブネット単位で特徴を抽出し，抽出した特徴を基にサブネットをクラスタリングすることによって外れ値のサブネットを検出して，攻撃元を推定するアノマリ型 IDS の手法を提案する．本手法では小さい処理コストで攻撃元を特定できる．

2 提案手法

2.1 特徴ベクトルの抽出

攻撃を検出するために，対象となるネットワークからトラフィックデータを収集し，単位時間で分割する．分割した各データから ttl や送信元 IP アドレス，宛先ポート番号など 64 種類の特徴量を抽出する．次にサブネット毎に特徴量をまとめ，各特徴量の値を平均が 0，分散が 1 になるように標準化する．その後，主成分分析を行い，累計寄与率が 80% となるまでの次元で特徴ベクトルを構成する．

2.2 クラスタリング

2.1 で抽出した特徴ベクトルは，類似した性質の通信を行っているサブネット間の距離は近く，類似しない通信を行っているサブネット間の距離は大きくなる．そこで，抽出した特徴ベクトルをクラスタリングすることにより，類似した性質の通信を行っているサブネットのクラスタを生成する．本研究では Mean-Shift 法を用いてクラスタリングを行う．この手法は分類するクラスタ数をあらかじめ指定する必要がなく，通信パターンの数が不明である場合に適した手法である．

2.3 異常検出

サイバー攻撃などの通信の特徴は，正常な通信とは異なると考えられる．また，サイバー攻撃等を行うサブネットは，正常な通信を行っているサブネットよりも少ないと考えられる．そこで，クラスタに属するサブネット数がしきい値 θ_1 より少ない場合，外れ値として抽出する．その後，外れ値のサブネットに最も近い正常クラスタ (メンバ数が θ_1 以上) を抽出して，外れ値のサブネットとクラスタ中心との距離を求め，求めた距離が θ_2 以上のサブネットを，サイバー攻撃等を行っている異常サブネットとして抽出する．

3 実験と考察

3.1 実験

本手法の有効性を確認するために，CICIDS2017[3] の火曜日から金曜日のデータセットを使用して実験を行った．攻撃元の IP アドレスは 1 種類であり，また曜日毎に攻撃の種類が異なっている．火曜日は FTP-Patator，SSH-Patator，水曜日は DoS 攻撃，木曜日は Brute Force, XSS, SQL Injection, 金曜日は Port Scan, Botnet，DDoS 攻撃が含まれており，それぞれの攻撃を行っているサブネットを正確に検出できることを確認する実験を行った．

ここで，サブネットは/16 で分割することとし，単位時間を 600 秒，しきい値 θ_1 を 3，しきい値 θ_2 を 25 として実験した．

* 大阪公立大学大学院情報学研究科 Graduate School of Informatics, Osaka Metropolitan University

表 1. 実験結果

火曜日	正常予測	異常予測
真の正常	13177(99.7%)	31(0.3%)
真の異常	2(14.2%)	12(85.8%)

水曜日	正常予測	異常予測
真の正常	13797(99.7%)	41(0.3%)
真の異常	3(21.4%)	11(78.6%)

木曜日	正常予測	異常予測
真の正常	13098(99.6%)	50(0.4%)
真の異常	3(37.5%)	5(62.5%)

金曜日	正常予測	異常予測
真の正常	12752(99.7%)	41(0.3%)
真の異常	1(9.0%)	10(91.0%)

3.2 結果

データセットに含まれる火曜日から金曜日のすべてのデータを単位時間で分割して，外れ値検出した結果を表 1 に示す．ここで真の異常とは，CICIDS2017 で公開されている攻撃時間を含む単位時間における攻撃元 IP アドレスを含むサブネットを示し，真の正常とはそれら以外の単位時間における各サブネットを示している．表 1 から火曜日は真の正常の 99.7% と真の異常の 85.8%，水曜日は真の正常の 99.7% と真の異常の 78.6%，木曜日は真の正常の 99.6% と真の異常の 62.5%，金曜日は真の正常の 99.7% と真の異常の 91.0% を正しく識別できたことを確認した．

火曜日から金曜日の全ての結果の中で異常として検出されたサブネットは 26 種類あった．異常と検出したサブネットの中で特に多かったものとそのサブネットの特徴量を調査した．異常サブネットである 172.16.0.0/16 は曜日や攻撃毎に違いはあるが，全ての曜日において送信元ポート番号の種類数が多く，水曜日や金曜日は 90% を占める単位時間も存在し，SYN 数や RST 数，PSH 数の割合も高くなっている．さらに木曜日と金曜日は宛先ポート番号の種類数も多くなっていた．全ての曜日において異常と誤検知した正常サブネットの多くは 172.217.0.0/16 であり，誤検知中の半数以上がこのサブネットだった．このサブネットは主に通信のあった IP アドレス数，PSH 数，TCP 数，宛先ポート番号の種類数が単位時間における他のサブネットの特徴量に比べて多くなっていた．他に 13.107.0.0/16 のサブネットも全ての曜日で異常と誤検知され，火曜日は 52.84.0.0/16 のサブネット，水曜日は 金曜日は 205.174.0.0/16 のサブネット等が異常として誤検知されていた．

3.3 考察

攻撃毎の検知率を表 2 に示す．DDoS は検知率は 100% となっており，DoS，Port Scan，FTP-Patator，SSH-Patator なども高い検知率となっている．異常を正常と誤識別した多くは，単位時間のはじめ，もしくは終わりの一部にのみ異常サブネットが存在し，パケット数が少なすぎるために外れ値とならず，検知できなかった場合だった．この場合の検知漏れを除いた場合，FTP-Patator，SSH-Patator，DoS，XSS の検知率は 100% だった．そして，SQL Injection については 1 つしかない攻撃の単位時間で検知できなかった．それ以外の Brute Force や Port Scan 等は単位時間のはじめ，終わりの一部以外にもに検知漏れが存在していた．

表 2. 主要な攻撃の検知率

攻撃名	検知数	誤検知数	検知率
FTP-Patator	6	1	85.7%
SSH-Patator	6	1	85.7%
DoS	10	1	90.9%
Heartbleed Port 444	1	3	25.0%
Brute Force	3	2	60.0%
XSS	2	1	66.7%
SQL Injection	0	1	0%
Port Scan	7	1	87.5%
DDoS	3	0	100%

正常を異常と誤検知した理由は，正常サブネットであっても単位時間内で大量の通信が行われることによってパケット数が増え，特徴量の数値が増えたために，外れ値として検知された場合だった．これらの解決方法としては，誤検知したサブネットの特徴が明らかになったため，この特徴に類似する特徴を持つサブネットを正常と判断するように設定するなどの方法が考えられる．

4 まとめ

本稿ではサブネット毎に 64 次元の特徴量を抽出して，抽出した特徴量を基にクラスタリングし，その外れ値により攻撃サブネットを検知する手法を提案した．実験では CICIDS2017 データセットを用いて本手法の有効性を確認した．今回の実験では，外れ値の個数のしきい値を 3 として実験したが，実環境では，異常サブネットが 3 以上ある場合も存在すると考えられるため，今後の課題としては，単位時間やしきい値等の最適値を自動的に探索する手法の検討などが挙げられる．

5 参考文献

[1] 佐藤陽平，和泉勇治，根本義章：複数の検出モジュールによるネットワーク異常検出の高精度化，信学技報，NS2004-144，pp.45-48(2004)
[2] 荒木翔平：通信のクラスタ間遷移に基づくサイバー攻撃検知手法，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015，No.3，pp.1066-1072
[3]Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018