Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

制御システムにおける多地点パケットキャプチャを利用した異常検知

西浩志[1]　布田裕一[2]　鈴木智道[3]　岡崎裕之[4]

概要：工場や発電所等の制御システムは，近年に入るまでインターネットに接続されない状態で運営されてきた．しかし，近年では，利便性を求めて汎用機器や TCP/IP 通信プロトコルなどが制御システムに導入されてきている．そのため，制御システムに対するセキュリティ対策が必須となっており，攻撃検知技術の重要性も高まっている．我々の研究では産業用プロトコル Modbus の偽装攻撃の検知を実施する．我々は原田らの用いた偽装攻撃，環境を 2 つのセグメントで再現して，OneClassSVM の結果に加えて IsolationForest による実験，評価を実施する．また，使用したデータセットをパターン化して 3 次元にすることで可視化して分析する．

キーワード：制御システム 偽造攻撃 機械学習 異常検知 OneClassSVM IsolationForest

Anomaly detection using Multipoint Packet Capture in Control Systems

KOUSHI NISHI[†1]　FUTA YUICHI[†2]
TOMOMI SUZUKI[†3]　TOSHIYUKI OKAZAKI [†4]

Abstract: Until recent years, control systems in factories and power plants have been operated without an Internet connection. However, in recent years, general-purpose devices and TCP/IP communication protocols have been used into the control systems in order to increase convenience. Therefore, it is necessary to take security measures for the control system. Attack detection techniques are also becoming increasingly important. We detect spoofing attacks on the industrial protocol Modbus. We reproduce two segments experimental environment used by Harada et al. We evaluate the results using IsolationForest and OneClassSVM. We also visualize and analyze the used dataset by making it patterned and three-dimensional.

Keywords: Control Systems　Spoofing Attack　machine learning　Anomaly detection　OneClassSVM　IsolationForest

1. はじめに

近年に入って，IoT 化や工場の機器の汎用化に伴って制御システムに対するサイバー攻撃も増加傾向にある．そのため，以前は独自の通信を使用していた制御システムにもセキュリティ対策が求められており，攻撃検知技術の重要性も高まっている．工場や発電所の制御システムのネットワークは主に 2 種類のネットワークで構成されている．1 つ目は,事務作業等を行っている情報ネットワークである．情報ネットワークでは，ファイヤーウォールを介してインターネットに接続されていることがある．汎用 OS による通信が行われているケースが多く，一般的に利用されている通信プロトコルが使われている．2 つ目は，工場の機器を制御・運用するための制御ネットワークである．制御ネットワークはモーターやタービン等のフィールド機器を制御するための特有の通信が求められる．情報ネットワークと制御ネットワークは,完全に分離されているわけでない．そのため，互いのネットワークで共有するデータや機器も存在する．そして，制御ネットワークでマルウェア感染させることで端末を支配する攻撃がある．マルウェアにネットワーク内をスキャンされることで，正常通信に似せた攻撃をされる事がある．そのため，工場ネットワークの攻撃検知では異なるネットワークに対する複数の攻撃を検知する必要がある．

2. 要素技術

2.1 制御システムのネットワーク

制御システムのネットワークはバッチ制御と連続制御の 2 種類がある．バッチ制御では，同一の整備や装置を使用して，製品の完成までの制御をするものである．原料の製造や，洗剤や食品の製造プラントが当てはまる．連続制御では，原料から製品にするまでの製造工程を連続的な物理化学的処理によって制御されるものである．石油精製プラントや製鉄所が当てはまる．汎用的な制御システムのネ

1 東京工科大学院バイオ情報メディア研究科
Tokyo University of technology Graduate School
Bionics,Computer and media science, Enterpreneurship program
Email: g2122031d7@edu.teu.ac.jp
2 東京工科大学コンピュータサイエンス学部
Tokyo University of technology
School of Computer Science
3 株式会社 PitApp
PitApp Inc
4 信州大学院 総合理工学研究科
Shinshu University Graduate School of Science and Technology

Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

ットワークの例を図 1 に示す．

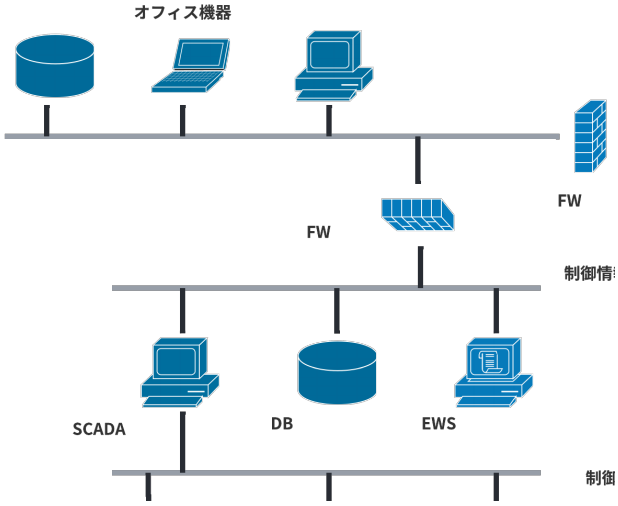

図 1 制御システムのネットワーク図

2.2 制御系の通信規則

制御系の通信は，オペレーターが SCADA や HMI を操作して，動作を指示することでフィールド機器に命令を与える．そして，フィールド機器からは PLC を通して，フィールド機器の状態である値が返ってくる．この動作を一定間隔で規則的に繰り返すことでオペレーターは全体の制御システムを監視する．

2.3 Stuxnet による攻撃

Stuxnet[3]は高度な標的型攻撃を行うために開発されたマルウェアである．ブシェール原子力発電のウラン濃縮施設を攻撃する際に使用され，遠心分離機のモーターが誤作動を起こした．ワームの様に端末から端末へ感染を拡大させる機能を持つ. USB 経由で制御システムに入り込み, PLC から制御プログラムを読み出し，不正コードを追加する．その後に, 制御プログラムを書き換えることで攻撃を行う．USB から制御システムに入り込む際は，Windows の脆弱性を利用している．

2.4 ClashOverride による攻撃

ClashOverride[4]はウクライナで発生した大規模停電が発生した際に使用されたマルウェアである．工業用制御システムで使用される作業プロセスを中断させる機能を持ち，変電装置のスイッチやブレイカーを直接制御できるように設計されている．バックドアを経由してランチャ機能やアタックツール，特定のプロトコルに対するペイロードとデータワイパコンポーネントをダウンロードして実際の攻撃を実施する．

2.5 アノマリー検知

制御システムに対する攻撃の検知手法は主に 2 つある．1 つ目はホワイトリストである．この手法はルールベースの検知手法となっており，あらかじめ複数ある正常な通信をリストに保存しておく．その後に，実際の通信を取得してホワイトリストと参照する事で，ホワイトリストに書いていない通信を検知する手法である．制御システムはあらかじめ定義された通信によって運用されているため，ホワイトリストによる検知が非常に有効である．

2 つ目は，アノマリー検知である．この手法は，あらかじめ正常な通信を定義しておき，正常通信から外れた通信を IDS や IPS を用いて検知する手法である．この手法で使う外れ値は閾値を用いる方法のほかに機械学習を用いる方法がある．本稿では，偽装攻撃に対して機械学習を用いたアノマリー検知を試みる．

2.6 偽装攻撃

工場ネットワークに対する攻撃には，制御システム特有の攻撃にカスタマイズされた制御ネットワークの通信による偽造攻撃がある．偽装攻撃は多くの場合，事前に攻撃対象の制御ネットワークに侵入して調査を行う．そして，調査結果をもとにネットワーク内の正常通信に似せた攻撃通信を定義する．偽装攻撃はルールベースのホワイトリストでは，防ぐことは難しい．あらかじめ制御システムの通信をマルウェアなどによって傍受して，正常通信に似せた通信を行っており，攻撃の通信がホワイトリストに登録されている場合があるためである．

2.7 機械学習による異常検知

機械学習による異常検知には教師無し学習を用いる．学習データには，正常通信と攻撃通信が混ざったデータを使用する．本研究では学習手法は OneClassSVM と IsolationForest を使用する． 本稿では，多地点からキャプチャした通信情報を OneClassSVM と IsolationForest によって学習させて，偽装命令に対する検知を行う．

2.8 ホワイトリストによる順序制約を用いた検知

藤田らは，順次制約を用いたホワイトリストによる異常検知を提案している[2]．HMI と PLC にそれぞれホワイトリストを導入している．HMI と PLC からパケットキャプチャを行い，そのパケットに対してホワイトリストを導入して検知を実施した．結果として，順序の動作や急停止などの異常は検知できた．しかし，正常な手続きの攻撃は検知できなかった．

2.9 制御系通信の OneClassSVM を用いた検知

原田らは，OneClassSVM を用いた Modbus/TCP のネットワーク異常検知を実施している[1]．仮想環境を構築して制御系通信のデータセットの作成方法を提案している. また，攻撃のシナリオとして正常通信に類似した攻撃通信の作成方法も提案している．攻撃通信を発生させるタイミングは完全にランダムであった．そして，OneClassSVM に学習させる前にデータの前処理を実施していた．その後，フィルタを使用して制御系通信のみを抜き出し，OneClassSVM を用いた検知を行った．結果は，偽装命令の攻撃を検知する事が可能であるとわかった．しかし，この手法では，過検知が生じることも判明した．

Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

3. 提案手法の概要

3.1 データセット作成方法

本稿では，正常時に利用する通信情報と類似する通信情報を用いた偽装攻撃を含めたデータセットを原田らのデータセット作成手法を用いて作成する．まず，OT ネットワーク内で行われる制御系の正常の通信を決めて学習用データセットを作成する．その後に，偽装攻撃が含まれるデータセットを作成する．正常時の通信を偽装する攻撃通信は制御系の通信である Modbus/TCP 通信のみを想定している．

3.2 検知手法

原田ら[1]の正常時の通信を偽装する攻撃を含めたデータセットの作成方法と正常時の通信を偽装する攻撃の提案手法を使用して 2 つのセグメントを持つ制御システムの仮想環境を構築する．その後，仮想環境で作成した多地点のパケットキャプチャによるデータセットを用いて，検知を実施する．

4. 提案手法の詳細と実験環境

本稿のデータセット作成を行うためのネットワークを示す．2 つのセグメントを持つネットワークを想定した．以下が，ネットワーク要件である．また，制御系通信の想定ネットワークを図 2 に示す．

・想定する制御：発電所などのバッチ制御を想定
・制御系通信：PLC から HMI，SCADA へのフィールド機器の状況を表示するための読み込み通信を実施する．
・SCADA：1 台の SCADA で 2 台の PLC の制御を実施する．
・HMI：1 台の HMI で 2 台の PLC の制御を実施する．
・PLC：フィールド機器を PLC によって制御する． 本稿では，フィールド機器は汎用的なものを想定しており具体的な想定はしていない．

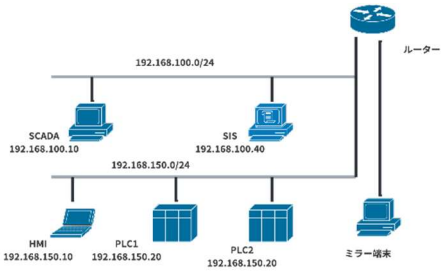

図 2 実験環境のネットワーク

4.1 通信パターン

正常と攻撃の通信を表 1 により示す．制御系通信は，SCADA と HMI からそれぞれ Read 命令が常に一定間隔で送られる．そして，任意のタイミングで PLC に対して Write 命令が単一で送られる．攻撃通信も同様に任意のタイミングで Write 命令の Batch 処理が一定間隔で送られる．

表 1 データセットの通信パターン

	送信元	送信先	通信内容	プロトコル	通信間隔	発生頻度
正常通信1	SCADA	PLC・SIS	Read 命令	Modbus/TCP	Batch 処理	常に
正常通信2	SCADA	PLC・SIS	Write 命令	Modbus/TCP	単一処理	稀に
正常通信3	HMI	PLC・SIS	Read 命令	Modbus/TCP	Batch 処理	常に
正常通信4	HMI	PLC・SIS	Write 命令	Modbus/TCP	単一処理	稀に
攻撃通信1	SCADA	SIS	Write 命令	Modbus/TCP	Batch 処理	稀に
攻撃通信2	SCADA	PLC	Write 命令	Modbus/TCP	Batch 処理	稀に
攻撃通信3	HMI	PLC	Write 命令	Modbus/TCP	Batch 処理	稀に

4.2 データセット

表 2 がデータセットの内訳を示したものである．各通信攻撃に対してデータセットを作成した．攻撃時データセットはすべて 45 分程度でキャプチャしたデータセットである．

表 2 データセットのパケット内訳

種類	総パケット数	攻撃パケット数	Modbus パケット数
正常時データセット	39899	0	5638
攻撃データセット 1	11065	170	1616
攻撃データセット 2	11612	154	1582
攻撃データセット 3	10339	134	1412

4.3 データセット可視化手法

データセットを送信元 IP アドレス，送信先 IP アドレス，送信元ポートをパターン化して三次元にデータを圧縮して可視化した．X 軸が時間差分，Y 軸が ModbusData，Z 軸がパターンである．

4.4 特徴量

原田らの検知手法[1]を使用して，OneClassSVM に学習さ

せるデータは，laytime，送信元 IP，宛先 IP，送信元ポート番号，宛先ポート番号，プロトコル，Modbus データの 7 つにする．laytime は制御系通信の通信間隔である．操作端末に偽装して，正常時の制御通信命令を上書きする動作に対する値となる．送信元 IP と宛先 IP は通信を行う機器同士の IP アドレスである．送信元ポート番号，宛先ポート番号は通信を行う機器同士のポート番号である．ポート番号はクライアント側の値を一致させるために置換を行う．プロトコルは通信を行う機器同士の通信プロトコルである．本研究では，Modbus/TCP と TCP の 2 種類のプロトコルを対象とする．Modbus データとは，Modbus のファンクションコードにより決まるフォーマットに従って，可変長のデータが格納される．以下に学習データを示す．

・laytime
・送信元/送信先 IP
・送信元/送信先ポート
・プロトコル
・ModbusData

4.5 制御系通信の多地点キャプチャ検知手法

2 つのセグメントで行われる制御系通信をキャプチャして, OneClassSVM, IsolationForest を用いた異常検知を行う．Python の機械学習ライブラリ Scikit-learn を使用して作成した OneClassSVM, IsolationForest によって制御系通信を抜き出して検知を実施する．その際に, Modbus/TCP によるパケットと通信間隔の情報を入力として使用する．

実際に OneClassSVM, IsolationForest に入力するデータとして，パケットの送信元 IP，宛先 IP，送信元ポート，宛先ポート，Modbus のファンクションコード，通信間隔に前処理を行ったデータを Numpy 配列に格納して学習を行う．また，データの正規化には Scikit-learn の StandardScaler を使用してモデル作成を実施した．

4.6 前処理

IP アドレス置換：事前に送信元 IP アドレスと送信先 IP アドレスの対をパターン化してリストに登録しておき，各パターンに対して等間隔で差配置し直す処理を実施した．

多地点 IP アドレス置換：多地点の場合は，IP アドレスのネットワークアドレスの第 3 オクテットとホスト部の第 4 オクテットの両方を見なければならない．しかし，機械学習のデータに独立していない特徴量を入れるわけにはいかないので，1 つの特徴量に圧縮するために，第 3 オクテットを 256 倍して第 4 オクテットを足したものを特徴量として使う方法があるが, 今回は IP アドレスの送信元と受信先をパターン化して等間隔で記録した．

ポート：クライアントポートはランダム化して学習を妨げる特徴量になるため，サーバポートのみ特徴量として使用する．

ModbusData：8 ビットで表される ModbusData を 10 進数に変換して特徴量に含める．

パターン化：送信元 IP アドレス，送信先 IP アドレス，送信元ポートをパターン化してリストに登録して起き，等間隔に配置し直す．データを可視化する際に三次元にデータを圧縮するために使用する．

4.7 学習方法

機械学習には Scikit-learn のライブラリを使用した．OneClassSVM，IsolationForest 共にデータセット 2 でパラメータ調整を実施した．そして，誤検知を 0 に調整したうえで，他のデータデータセットに対して検知を行った．

4.8 検知結果

各データセットに対して OneClassSVM と IsolationForest でパラメータ調整をした後に検知を実施した結果を混合行列で表 3，5 にまとめた．また，混合行列から，正解率・精度・再現率を表 4，6 にまとめた．

表 3 OneClassSVM の混合行列

利用情報	TP	TN	FP	FN
攻撃データセット 1	1410	170	0	54
攻撃データセット 2	1416	157	0	27
攻撃データセット 3	1262	135	0	30

表 4 OneClassSVM の検知結果

利用情報	正解率 (Accuracy)	精度(Precision)	再現率 (Recall)
攻撃データセット 1	0.967	1.0	0.9631
攻撃データセット 2	0.9831	1.0	0.9812
攻撃データセット 3	0.978	1.0	0.9768

表 5　IsolationForest の混合行列

利用情報	TP	TN	FP	FN
攻撃データセット 1	1225	170	0	239

Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

攻撃データセット 2	1129	135	0	163
攻撃データセット 3	1262	157	0	181

表 6　IsolationForest の検知結果

利用情報	正解率 (Accuracy)	精度 (Precision)	再現率 (Recall)
攻撃データセット 1	0.8537	1.0	0.8367
攻撃データセット 2	0.8857	1.0	0.8738
攻撃データセット 3	0.8869	1.0	0.8746

4.9 検知結果の可視化

使用した特徴量を 3 次元にして検知結果に色を付けて可視化した．左斜め前を正面として左手系で X 軸が時間差分，Y 軸が ModbusData，Z 軸がパターンである．青が TN，赤が FP，緑が TP，黄が FN である．各データセットに対して OneClassSVM の検知を可視化したものが図 3，4，5 である．IsolationForest で検知したものが図 6，7，8 である．

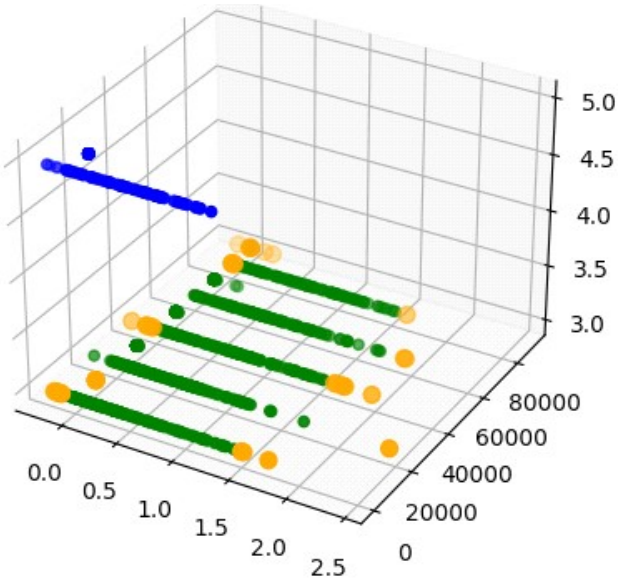

図 3 データセット 1：OneClassSVM の検知結果

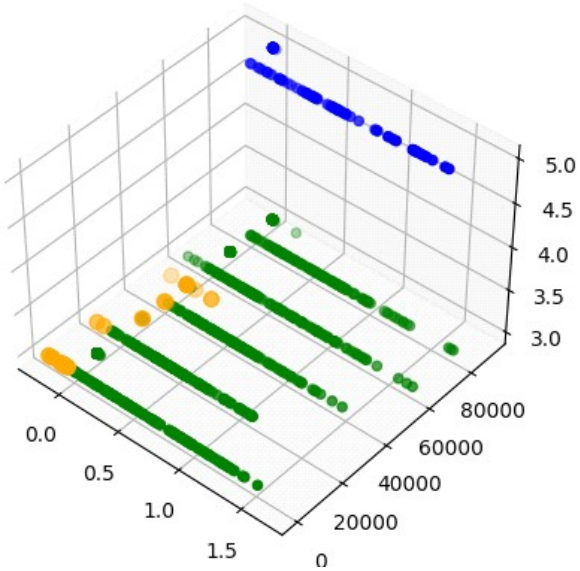

図 4 データセット 2：OneClassSVM の検知結果

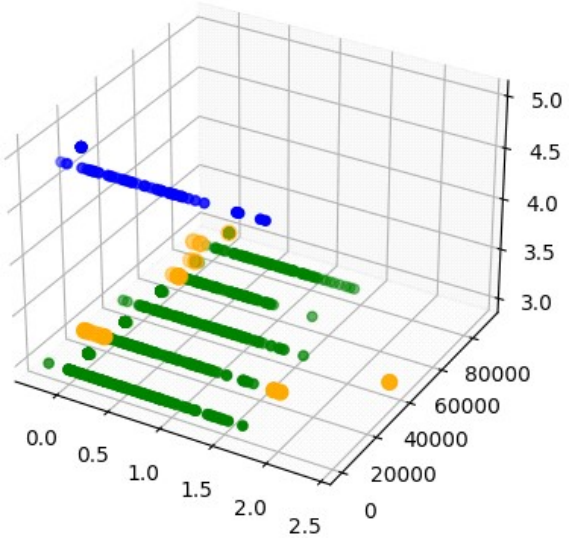

図 5 データセット 3：OneClassSVM の検知結果

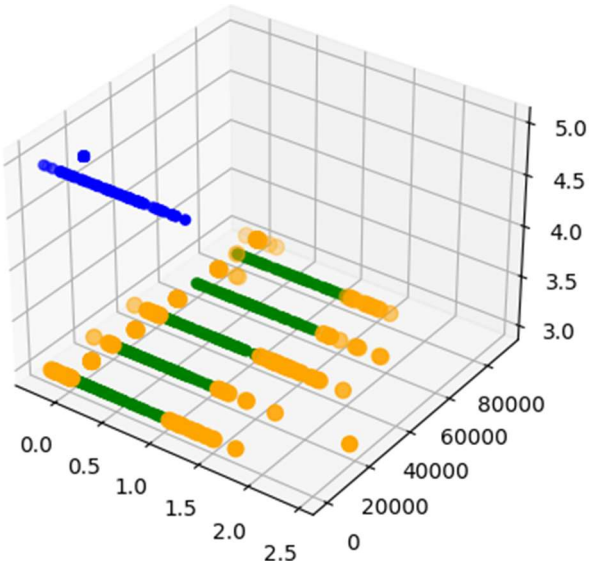

図 6 データセット 1：IsolationForest の検知結果

Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

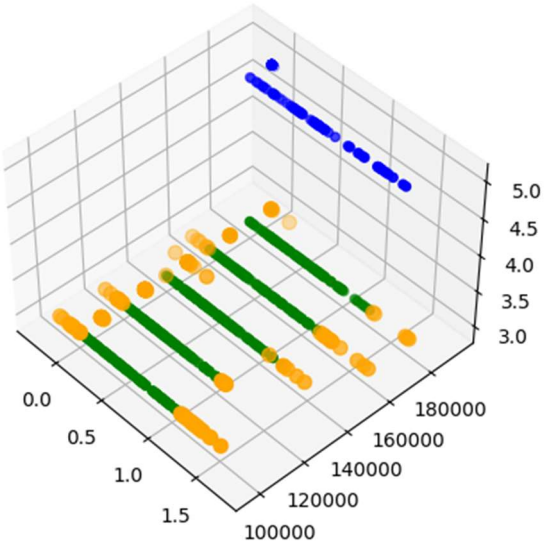

図 7 データセット 2：IsolationForest の検知結果

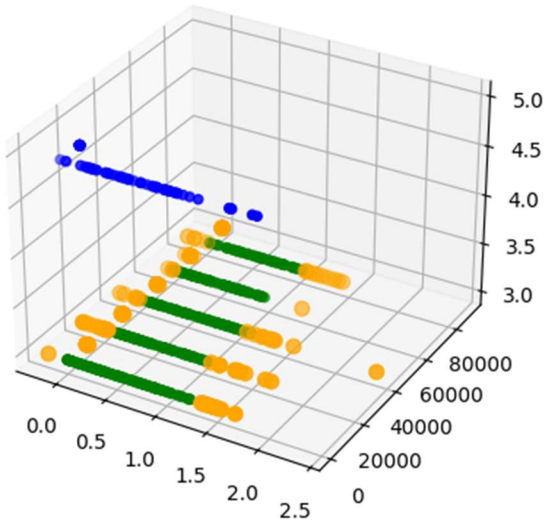

図 8 データセット 3：IsolationForest の検知結果

5. 考察

多地点から取った制御系通信のパケットに対して，OneClassSVM を用いた検知でも，偽装命令を行う様な攻撃の検知はできることがわかった．また，原田らの研究では，1 つのセグメントで実験をした結果，正解率が 0.794142，精度が 0.744888 であった．これはパラメータ調整に大きく検知結果が依存すると考えられる．学習データとしては IP アドレスのパターンが増えただけであるため，パターンが増えた分パラメータ調整が難しくなっていると考えるが，Scikit-learn によるパラメータ調整が行いやすいデータセットであった可能性も考えられる．

時間差分を見ると一定間隔で送られているはずの正常通信にかなりのばらつきがある．これは，攻撃によるものだと考える．しかし，実験環境によるものである可能性もある．バッチ処理と単一処理の時間差分の変化から偽装攻撃を高精度で検知できると考えていたが，攻撃通信が時間差分に与える影響が大きいため，高精度の検知が難しいことがわかった．解決策として，パターン化した通信ごとに差分を取る事で最初に意図していた時間の変位を正確に記録できると考える．また，ノイズが入る次元データに対しては，前処理によるユークリッド距離の引き延ばしによってある程度は対処できると考える．

IsolationForest はパラメータ調整をしなくてもはじめから高い精度の検知結果が出力された．これは，OneClassSVM に比べてアルゴリズム内で入力データに対して沿うように学習をしているものだと考える．そのため，偽装攻撃のような比較的に正常と攻撃データが似通った場合は，IsolationForest の方が有効な手段であると考える．また，偽装攻撃はデータが似ており，分離境界を細かく設定する必要があるため，パラメータ調整も詳細に行う必要がある．OneClassSVM はパラメータ調整を続ければ精度を上昇は可能であると考えるが，Scikit-learn よりもさらに詳細にパラメータ調整を行える実装が求められる．

今回は，アノマリー検知の強みを生かすために特徴量のすべてを学習に使用したが，偽装攻撃の変位が出る特徴次元が判明している際は，その次元のみを抽出して行う方が精度の上昇も見込め，パラメータ調整も簡単だと考える．

今回は攻撃データセットに Modbus の Write 命令による通信が含まれないことが前提にあったため，OneClassSVM も IsolationForest も ModbusData での分離をするように学習させる必要があった．しかし，実際は攻撃データセット内にも正常データとして Write の通信が単一で流れていると考えられる．その場合は，時間差分のみを手掛かりに検知する必要があるため，今回の検知手法では高精度の検知は難しいと考える．対抗策として，通信をパターン化して時間差分を取ることである程度攻撃による時間差分の攪乱を防ぐことができると考える．

6. まとめ

6.1 まとめ

原田ら[1]のデータセット作成手法と検知手法を用いて多地点キャプチャによる検知を行った．検知結果は，OneClassSVM，IsolationForest ともに 1 地点よりも高い精度を出すことができた．しかし，これがデータによるものなのか，パラメータ調整によるものなのかがわからない．

偽装攻撃における OneClassSVM と IsolationForest を比べると結果的には OneClassSVM の方が高精度なものとなったが，これはパラメータ調整をより詳細に行ったものであり，IsolationForest の方がパラメータ調整しなくても高精度な検知結果を出せることがわかった．

6.2 今後の課題

今回は偶然パラメータ調整が成功した結果，高精度な検知結果を出すことが出来たが，今後は各手法の有効性を比

Vol.2022-CSEC-99 No.8
Vol.2022-SPT-49 No.8
Vol.2022-EIP-98 No.8
2022/12/22

較するためにもパラメータ調整の方法を統一化して検知を実施する必要がある．

また，今回高精度の検知結果を出せたのはModbusDataによる分離が可能だったからである．そのため，時間差分のみに特徴が表れる偽装攻撃を検知できたとは言いにくい．時間差分のみ特徴が表れる偽装攻撃を検知するためには，テストデータセットに単一の Write 通信がある事を仮定して検知精度を上げなければならない．

多地点によるパケットキャプチャが効果的である根拠は本稿では示せなかった．そのため，多地点で連携する攻撃を試して，一地点との比較する事で，多地点検知の有効性を示す必要がある．

謝辞 本研究の一部は，JSPS 科研費 JP22K11982 の助成を受けたものです．

参考文献

[1] 藤田真太郎，澤田賢治，”通信パケットの順序制約を考慮した制御ネットワークのホワイトリスト”，SCIS2020，3D1-5，2020.
[2] 原田雄基，布田裕一，“SVM を用いた制御システムに対する偽装命令攻撃の検知”，信学技報，Vol. 121，No. 118，ISEC2021-15，pp. 35-40，2021 年 7 月．
[3] “IPA 制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ Stuxnet:制御システムを標的とする初めてのマルウェア”，https://www.ipa.go.jp/files/000080701.pdf ，(参照 2021-6-31).
[4] “IPA 制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ 2016 年ウクライナマルウェアによる停電”，https://www.ipa.go.jp/files/000076756.pdf，(参照 2021-6-31).