SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

SVMによる工場ネットワークにおける偽装通信の検知手法のリアルタイム性の検証

Evaluation of the Real-time Performance of Detection of Fake Communication over Factory Networks using SVM

原田　雄基 * 布田　裕一 † 岡崎 裕之 ‡
Yuki Harada Yuichi Futa Hiroyuki Okazaki

キーワード キーワード 制御システム，攻撃検知，One Class SVM，リアルタイム性

あらまし

工場やプラントなどの制御システムは，従来インターネットには接続されていないクローズドな環境であったため，セキュリティ上の脅威に対してあまり考慮されていなかった．しかし，近年のデータ公開に対するニーズの高まりや利便性を求め，制御システムにおいてもWindowsやLinuxなどの汎用製品，TCP/IP通信プロトコルなどが導入されてきている．そのため，それらの技術に対する攻撃が制御システムにおいても発生するリスクが高まってきている．そのため，制御システムにおいてもセキュリティ上の脅威の対策が必要となってきている．さらに，制御システムを含む工場等の施設においては，情報システムと異なり可用性を重視したセキュリティ対策が必須である．そのため，セキュリティソフトなどの構成機器に対策を加えるアクティブな対応ではなく，通常の動作に影響を与えないパッシブな情報収集を行うことが必要である．その情報を用いた異常検知などの対策が重要となっている．しかし，パッシブな情報収集による異常検知において検知時間が長くなると実際の生産システムに影響が出る前に検知することができない．工場に対するセキュリティ対策では，リアルタイム性も重要となる．

我々は，工場を対象とする攻撃検知手法の評価のために工場ネットワークを想定し，正常時の通信と類似する通信を用いたデータセットを作成した[1]．また，制御系通信で行われる偽装命令による攻撃を想定し，IPアドレスなどのヘッダー情報によるフィルタとペイロード情報を用いたOne Class SVMの検知手法の提案を行った[2]．

本稿では，提案手法であるフィルタとOne Class SVMを用いた検知手法において受信パケットの判定にかかる時間を測定し，リアルタイム性の検証を行う．受信パケットの判定では，ポート番号などによるフィルタによって検知が可能であるポートスキャンなどの正常時では通信に利用されない情報を利用する攻撃，One Class SVMを用いて検知を行う正常時も利用される情報を用いた偽装命令攻撃を想定し，提案手法において受信した1パケットの異常判定にかかる時間を測定する．また，実際に工場ネットワークで動作することを想定し，正常時通信と攻撃通信が連続して提案手法に入力した場合の時間を測定する．

参考文献

[1] 原田雄基，布田裕一，岡崎裕之，”制御システムにおける異常検知手法とデータセットの評価”,SCIS 2021, 3E4-2,2021

[2] 原田雄基，布田裕一，岡崎裕之，”SVMを用いた制御システムに対する偽装命令攻撃の検知”，ISEC2021,2021年7月

* 東京工科大学大学院　バイオ・情報メディア研究科コンピュータサイエンス専攻〒 192-0982 東京都八王子市片倉町 1404-1., Tokyo University of Technology Graduate School, 1404-1, Katakuramachi, Hachioji City, Tokyo, 192-0982, JAPAN.
† 東京工科大学　コンピュータサイエンス学部〒 192-0982 東京都八王子市片倉町 1404-1. Tokyo University of Technology Department of Computer Science , 1404-1, Katakuramachi, Hachioji City, Tokyo, 192-0982, JAPAN.
‡ 信州大学 学術研究院 (工学系) 〒 380-8553 長野県長野市若里 4-17-1. Faculty of Engineering, Shinshu University 4-17-1, Wakasato, Nagano City 380-8553, JAPAN.