ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

Modelling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach

[1] K VENKATESH, [2]P.MANOJ KUMAR

(Assistant Professor), MSC, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

[2]MSC, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

ABSTRACT

The rise of the Internet of Medical Things introduces the healthcare ecosystem in a new digital era with multiple benefits, such as remote medical assistance, realtime monitoring, and pervasive control. However, despite the valuable healthcare services, this progression raises significant cybersecurity and privacy concerns. In this article, we focus our attention on the IEC 60 870-5-104 protocol, which is widely adopted in industrial healthcare systems. First, we investigate and assess the severity of the IEC 60 870-5-104 cyber attacks by providing a quantitative threat model, which relies on Attack Defence Trees and Common Vulnerability Scoring System v3.1. Next, we introduce an intrusion detection and prevention system (IDPS), which is capable of discriminating and mitigating automatically the IEC 60 870-5-104 cyberattacks. The proposed IDPS takes full advantage of the machine learning (ML) and software defined networking (SDN) technologies. ML is used to detect the IEC 60 870-5-104 cyberattacks, utilizing

1) Transmission Control Protocol/Internet Protocol network flow statistics and

2) IEC 60 870-5-104 payload flow statistics.

1.INTRODUCTION

THE rapid evolution of the Internet of Medical Things (IOMT) leads the healthcare ecosystem to a new digital paradigm with valuable services, such as remote monitoring, faster diagnosis, preventive care, and health education. Based on the current situation of the COVID-19 pandemic and future pandemics, this evolution and, in general, the complete digitization of the healthcare cyber–physical infrastructures become more necessary than ever. However, despite the benefits, this new reality raises crucial cyber security and privacy risks due to the sensitive nature of the healthcare data and the vulnerabilities of the involved entities [1]. In particular, the healthcare sector is considered as the most sensitive critical infrastructure (CI) in terms of cyber security due to the vast amount of personal and administrative data aggregated in electronic health record applications. A characteristic healthcare-related cyber security incident was the WannaCry ransom ware, which paralyzed the United Kingdom's National Health Service in May 2017.

Therefore, based on the aforementioned remarks, the presence of reliable intrusion detection and prevention mechanisms is vital. In this article, we focus our attention on the IEC 60 870-5-104 protocol, which is widely adopted by industrial healthcare systems [2]. IEC 60 870-5-104 is characterized by severe cyber security issues since it does not include adequate authentication and authorization mechanisms. Thus, it allows potential cyber attackers to perform various cyber-attacks like Denial of Service (DOS) and unauthorized access. Such cyber-attacks against IEC 60 870-5-104 can lead to devastating consequences in the healthcare ecosystem. Moreover, it is noteworthy that IEC 60 870-5-104 is used by other CIs, such as the energy domain. Consequently, possible IEC 60 870-5-104 cyber-attacks can lead to cascading effects among different CIs. First, this article investigates the criticality of the IEC 60 870-5-104 cyber-attacks by introducing a quantitative threat model, which combines an Attack Defence Tree (ADT) and the Common Vulnerability Scoring System (CVSS) v3.1. Next, we provide an intrusion detection and prevention system (IDPS), which takes advantage of the machine learning (ML) and software defined networking (SDN) technologies. ML is used to detect the IEC 60 870-5-104 cyber-attacks, utilizing 1) Transmission Control Protocol (TCP)/Internet Protocol (IP) network flow statistics and 2) IEC 60 870-5-104 payload flow statistics. On the other side, the automated mitigation is transformed into a multi armed bandit (MAB) problem, which is solved through a reinforcement learning (RL) method called Thomson sampling (TS) and SDN. Hence, the contributions of this article are summarized as follows.

1) Providing a quantitative IEC 60 870-5-104 threat model: The proposed threat

model determines the severity of the IEC 60 870-5-104 cyberattacks, combining ADT and CVSS v3.1.

2) Detecting IEC 60 870-5-104 cyber-attacks:We provide an ML-based IDPS capable of detecting accurately the IEC 60 870-5-104 cyber-attacks. Due to the lack of available IEC 60 870-5-104 datasets, a new IEC 60 870-5-104 intrusion detection dataset is implemented and provided in the context of this work.

3) Mitigating automatically IEC 60 870-5-104 cyber-attacks: The automatic mitigation is transformed into a MAB problem, which is solved through TS and SDN. TS is responsible for the decision-making process, while SDN

undertakes to apply the mitigation strategy.

The rest of this article is organized as follows. Section II discusses relevant works. Section III presents the quantitative IEC 60 870-5-104 threat model. Section IV describes the architecture of the proposed IDPS, focusing mainly on the detection of the IEC 60 870-5-104 cyberattacks. Section V analyses the mitigation process. Section VI is devoted to the evaluation results. Finally, Section VII concludes this article.

2. EXISTING SYSTEM

Several papers have investigated the cybersecurity issues in the healthcare sector. Some of them are listed in [1], [9]– [13]. In particular, in [1], Yaqoob et al. investigate the vulnerabilities of the smart medical devices and propose appropriate countermeasures. In [9], Chanthira et al. discuss the cybersecurity and privacy challenges of the e-health solutions in cloud-computing environments. Similarly, Walker-Roberts et al. [10] discuss relevant countermeasures against internal threats in healthcare CIs.

Vijayakumar et al. [11] provide an anonymous authentication framework for wireless body area networks. Finally, Sun et al. [12] provide a detailed survey about the IoMT security and privacy issues. Next, we elaborate on some similar works regarding 1) IEC 60 870-5-104 threatmodelling, 2) detecting intrusions against IEC 60 870-5-104, and 3) mitigating or even preventing cyberattacks through SDN.

In [5], the authors conduct an abstract threat analysis of the IEC 60 870-5-104 industrial systems. Based on a coloured Petri net (CPN) analysis, two cyberattack categories are specified: 1) physical attacks and 2) cyberattacks. The first category denotes those activities performed by an attacker having physical access to the target system. On the other side, the cyberattacks refer to those that exploit the IEC 60 870-5-104 vulnerabilities. In particular, based on the authors, the second category includes the following four kinds:

1) unauthorized access;

2) man-in-the-middle (MITM);

3) DoS;

4) traffic analysis.

Each of the aforementioned cyberattacks is assigned to the CPN transitions. Next, the authors emulate the four IEC 60 870- 5-104 cyberattacks and quantify their risk based on the Alien- Vault OSSIM risk model.

Hodo et al. [3] adopt various ML algorithms to detect cyberattacks against an emulated industrial environment using the IEC 60 870-5-104 protocol. To this end, the authors use a dataset consisting of 1) replay attacks, 2) DoS attacks, and (c) address resolution protocol spoofing attacks. Thus, they evaluate the classification performance of various ML classifiers, including Random Forest, OneR, J48, IBk, and Naive Bayes.

According to the evaluation results, J48 achieves the best performance. Yang et al. [4] create Snort-compliant signature and specification rules to detect IEC 60 870-5-104-related cyberattacks. The difference between the signature and specification rules lies in the fact that the former category defines malicious patterns, while the second determines the normal behaviour. The same authors in [7] introduce a specification-based intrusion detection system (IDS) capable of recognizing IEC 60 870-5-104 anomalies. The proposed IDS relies on a detection state machine, which relies on finite state machines. The experimental results confirm the efficiency of the proposed IDS.

3. PROPOSED SYSTEM

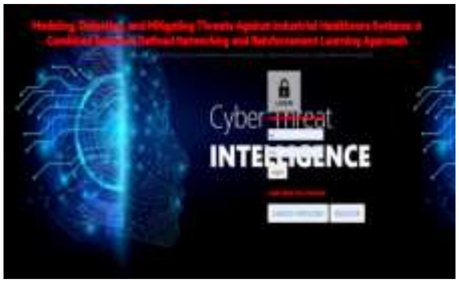
The proposed IEC 60 870-5-104 threat modelling combines both ADT and CVSS that determine the cyberattack paths and their risks, respectively. In particular, an ADT [16] comprises two antagonistic nodes: 1) attacking nodes and 2) defending nodes. The attacking nodes describe the goal and the actions that a cyberattacked may adopt in order to compromise the security of the target system. The defending nodes correspond to the defences that can be used by the defender in order to address or mitigate a cyberattack.

Each node can have one or more children of the same type (i.e., attacking node or defending node), thus reflecting a refinement into specific sub goals and actions. If a node does not have any refinement (i.e., children of the same type), then it constitutes a non refunded node, which indicates a basic action. Moreover, a node can have children of the opposite type, thus defining a countermeasure.

A refinement can be classified into two types: 1) conjunctive and 2) disjunctive. In the first case (i.e., conjunctive refinement), the goal of a refined node is achieved, whether all of its children accomplish their goals. Thus, a conjunctively refined node is characterized by an AND operator. On the other side, a disjunctively refined node is characterized by an OR operator, i.e., its goal is achieved if at least one of its children achieves its goal. On the other side, CVSS is an open vulnerability assessment framework, which quantifies the severity of each vulnerability or attack between 0 and 10 [17].

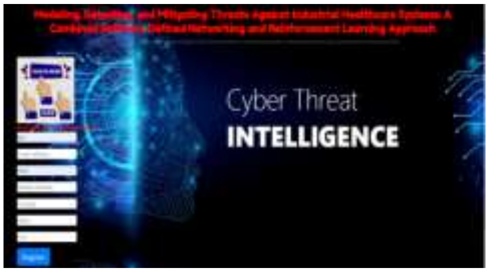
4. OUTPUTSCREENS

Login Page:



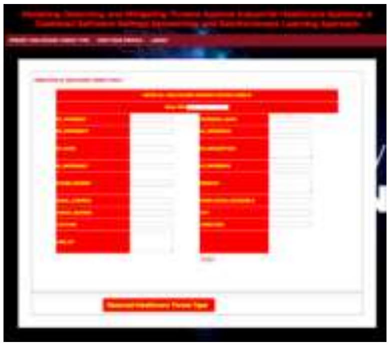
Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach

Registration Page:

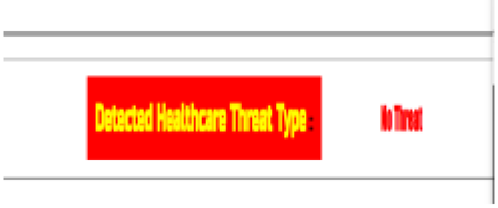


Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach

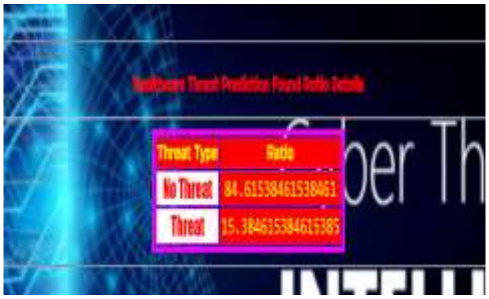
Predict Health care Threat type



View output for provided details



Detected Healthcare Threat Type No Threat

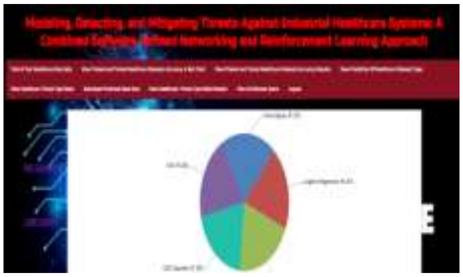


Healthcare Threat Prediction Found Ratio Details

Threat Type	Ratio
No Threat	84.61538461538461
Threat	15.384615384615385

Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach

Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach



Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach

5. CONCLUSION

Despite the necessary digitization of the healthcare ecosystem, the IoMT progression and mainly the insecure nature of the legacy healthcare systems increases the attack surface.

In this article, we paid our attention to the IEC 60 870-5-104 protocol, which is widely adopted by the industrial systems in the healthcare sector. In particular, first, we introduced a quantitative threat model, which evaluates the severity of the possible cyber-attacks with respect to the corresponding IEC 60 870-5-104 commands. Next, we provided an IDPS system, which combines ML and SDN in order to detect and mitigate the IEC 60 870-5-104 cyber-attacks. The intrusion detection relies on a CART classifier that uses the TCP/IP network flow statistics and IEC 60 870-5-104 payload flow statistics. On the other side, the SDN-based mitigation is transformed into a MAB problem solved with the TS method. The evaluation results demonstrated the efficiency of the proposed IDPS. Our future plans related to this work are focused on enhancing the proposed IDPS so that it can detect multistep cyber-attacks related to IEC 60 870-5-104 and other industrial and IOMT protocols utilized in the healthcare sector, such as Mod bus, MQTT, and Ether CAT. To this end, ML-based association rules techniques will be adopted.

6. REFERENCE

[1] T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—

A review,” IEEE Commun. Surv. Tut., vol. 21, no. 4, pp. 3723–3768, Oct./Dec. 2019.

[2] M.Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," 2021, arXiv:2102.05631.

[3] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," in Proc. 12th Int. Conf. Availability, Rel. Secur., 2017, pp. 1–7.

[4] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in Proc. IEEE Power Energy Soc. Gen.Meeting, 2013, pp. 1–5.

[5]P.Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis,E.Kafetzakis, andE. Panaousis, "Attacking IEC-60870-5-104SCADAsystems," in Proc. IEEE World Congr. Serv. (SERVICES), 2019, pp. 41–46.

[6] P. R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, and G. Efstathopoulos, "An anomaly detection mechanism for IEC 60870-5-104," in Proc. 9th Int. Conf. Modern Circuits Syst. Technol., 2020, pp. 1–4.

[7] Y. Yang, K. McLaughlin, S. Sezer, Y. Yuan, and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," in Proc. IEEE PES Gen. Meeting Conf. Expo., 2014, pp. 1–5.

[8] P. Radoglou-Grammatikis et al., "Spear SIEM: A security information and event management system for the smart grid," Comput. Netw., vol. 193, 2021, Art. no. 108008.

[9] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-health solutions in cloud computing," IEEE Access, vol. 7, pp. 74361–74382, 2019.
[10] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," IEEE Access, vol. 6, pp. 25167–25177, 2018.