IEEE Transactions on Industrial Informatics,Volume:18,Issue:3,Issue Date:March.2022

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

Panagiotis Radoglou-Grammatikis, *Member, IEEE*, Konstantinos Rompolos, Panagiotis Sarigiannidis, *Member, IEEE*, Vasileios Argyriou, Thomas Lagkas, Antonios Sarigiannidis, Sotirios Goudos, *Senior Member, IEEE*, and Shaohua Wan, *Senior Member, IEEE*

***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, real-time 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 cyberattacks 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. On the other side, the automated mitigation is transformed into a multiarmed bandit problem, which is solved through a reinforcement learning method called Thomson sampling and SDN. The evaluation analysis demonstrates the efficiency of the proposed IDPS in terms of intrusion detection accuracy and automated mitigation performance. The detection accuracy and the F1 score of the proposed IDPS reach 0.831 and 0.8258, respectively, while the mitigation accuracy is calculated at 0.923.**

***Index Terms*—Cybersecurity, IEC 60 870-5-104, Internet of Medical Things (IoMT), intrusion detection, machine learning (ML), reinforcement learning (RL), software defined networking (SDN).**

Manuscript received February 25, 2021; revised May 24, 2021; accepted June 17, 2021. Date of publication July 1, 2021; date of current version December 6, 2021. This work was supported by the European Union's Horizon 2020 research and innovation program under Grant 833955. Paper no. TII-21-0949. *(Corresponding author: Shaohua Wan.)*

Panagiotis Radoglou-Grammatikis, Konstantinos Rompolos, and Panagiotis Sarigiannidis are with the Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece (e-mail: pradoglou@uowm.gr; krobolos@uowm.gr; psarigiannidis@uowm.gr).

Vasileios Argyriou is with the Department of Networks and Digital Media, Kingston University London, KT1 2EE Kingston, U.K. (e-mail: vasileios.argyriou@kingston.ac.uk).

Thomas Lagkas is with the Department of Computer Science, International Hellenic University, 65404 Thermi, Greece (e-mail: tlagkas@cs.ihu.gr).

Antonios Sarigiannidis is with Sidroco Holdings Ltd, Nicosia 1077, Cyprus (e-mail: asarigia@sidroco.com).

Sotirios Goudos is with the School of Physics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece (e-mail: sgoudo@physics.auth.gr).

Shaohua Wan is with the School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan 430073, China (e-mail: shwanhust@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3093905.

Digital Object Identifier 10.1109/TII.2021.3093905

I. 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 cybersecurity 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 cybersecurity due to the vast amount of personal and administrative data aggregated in electronic health record applications. A characteristic healthcare-related cybersecurity incident was the `WannaCry` ransomware, 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 cybersecurity issues since it does not include adequate authentication and authorization mechanisms. Thus, it allows potential cyberattackers to perform various cyberattacks like Denial of Service (DoS) and unauthorized access. Such cyberattacks 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 cyberattacks can lead to cascading effects among different CIs. First, this article investigates the criticality of the IEC 60 870-5-104 cyberattacks 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 cyberattacks, 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 multiarmed 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 cyberattacks: We provide an ML-based IDPS capable of detecting accurately the IEC 60 870-5-104 cyberattacks. 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 cyberattacks: 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 analyzes the mitigation process. Section VI is devoted to the evaluation results. Finally, Section VII concludes this article.

II. Related Work

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], Chenthara *et al.* discuss the cybersecurity and privacy challenges of the e-health solutions in cloud-computing environments. Similarly, Wolker-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 threat modeling, 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 colored 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 `AlienVault 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 behavior. 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.

Lin [14] introduces an SDN-based in-network honeypot, which can mitigate the impact of a cyberattack by 1) isolating the cyberattacker and 2) spoofing the network communication, thereby establishing a connection with a cyberattacker via nonexistent nodes, called phantom nodes. This connection allows the defender to mislead the cyberattacker and gather useful information. Initially, the SDN controller (SDN-C) quarantines the malicious nodes by corrupting their communication with any legitimate node. Next, the SDN-C uses spoofed IP addresses that communicate with the cyberattacker by adapting appropriately

TABLE I
COMPARISON WITH RELEVANT WORKS

Reference	Threat Modeling	Anomaly Detection	Cyberattack Discrimination	Cyberattack Mitigation
E. Hodo et al. [3]	✓	✓	X	X
Y. Yang et al. [4]	X	X	✓	X
P. Radoglou-Grammatikis et al. [5]	✓	X	X	X
P. Radoglou-Grammatikis et al. [6]	X	✓	X	X
Y. Yang et al. [7]	X	✓	X	X
SPEAR SIEM [8]	X	✓	✓	X
Proposed IDPS	✓	✓	✓	✓

the network packets' content at the network and application layers. To this end, statistic and physical models are utilized, respectively.

Xing *et al.* [15] present an SDN-based intrusion prevention system (IPS) called SDNIPS. The SDNIPS architecture consists of the following four modules:

1) `Snort` agent;
2) SDNIPS daemon;
3) alert interpreter;
4) rules generator.

The `Snort` agent is responsible for detecting the potential cyberattacks by applying the respective signature rules. Next, the SDNIPS daemon undertakes to transform the detection results into a JavaScript Object Notation (JSON) format, which is transmitted to the SDN-C. The alert interpreter processes the JSON files, thus extracting the appropriate information, such as the IP addresses. Finally, the rule generator produces the OpenFlow entries introduced into the `Open vSwitch` flow tables. The authors evaluate their IPS with a typical IPS relying on `iptables`. The evaluation criterion is whether both IPS can generate alerts under tremendous network traffic conditions. To this end, two DoS attacks are emulated. The proposed IPS exceeds the performance of the typical IPS using `iptables`.

Undoubtedly, the aforementioned works provide useful and significant insights. Table I compares the previous, similar works with respect to the following:

1) IEC 60 870-5-104 threat modeling;
2) IEC 60 870-5-104 anomaly detection;
3) IEC 60 870-5-104 cyberattack discrimination;
4) IEC 60 870-5-104 cyberattack mitigation.

Apart from the aforementioned works, Table I contains also [6] and [8] that provide an IDS and a security information and event management (SIEM) system for IEC 60 870-5-104, respectively. As depicted, most of the current works cannot discriminate the various IEC 60 870-5-104 cyberattacks and mitigate them. In particular, they do not consider 1) the various cyberattacks depending on the IEC 60 870-5-104 commands and 2) the sensitive nature of the CIs, such as the industrial healthcare systems. Regarding the first key point, this article provides a quantitative threat model, taking into account the IEC 60 870-5-104 commands. Moreover, the proposed IDPS can discriminate precisely the various cyberattacks with respect to the IEC 60 870-5-104 commands. On the other side, although the existing works demonstrate how SDN can mitigate the possible intrusions, they do not take into account that the automated countermeasures (such as the isolation of the compromised assets in a sensitive environment) can lead to more devastating consequences. To this end, in this article, we formulate the mitigation decision as a MAB problem, which is solved with the TS method.

III. IEC 60 870-5-104 THREAT MODELING

The proposed IEC 60 870-5-104 threat modeling 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 cyberattacker 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 subgoals and actions. If a node does not have any refinement (i.e., children of the same type), then it constitutes a nonrefined 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].

Fig. 1 depicts the ADT of the proposed IEC 60 870-5-104 threat analysis. In our analysis, we have considered the nonrefined nodes as IEC 60 870-5-104 cyberattacks supported by existing attacking tools, such as the `Metasploit` framework (i.e., auxiliary/client/iec104/iec104), `Qtester104`, `OpenMUC j60870`, `IEC-TestServer`, and custom `Ettercap` filters. Therefore, the nonrefined nodes are the following:

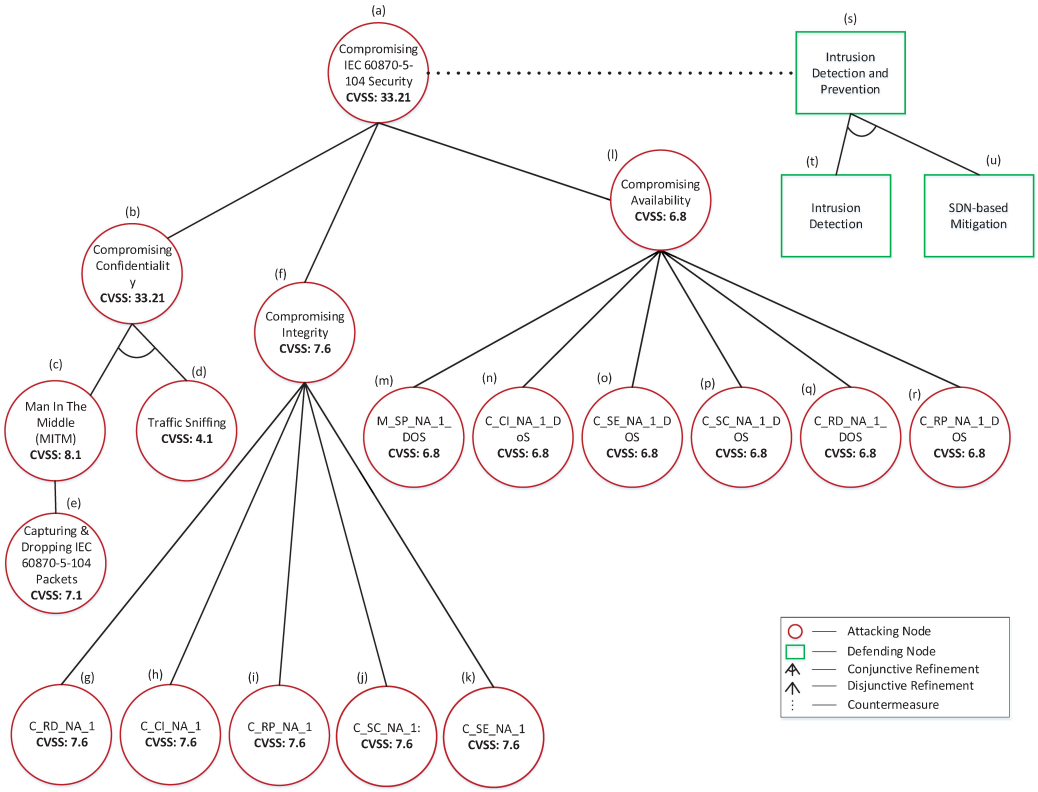


Fig. 1. Proposed IEC 60 870-5-104 ADT.

1) MITM;
2) traffic sniffing;
3) C_RD_NA_1;
4) C_CI_NA_1;
5) C_RP_NA_1;
6) C_SC_NA_1;
7) C_SE_NA_1;
8) M_SP_NA_1_DOS;
9) C_CI_NA_1_DOS;
10) C_SE_NA_1_DOS;
11) C_RD_NA_1_DOS;
12) C_RP_NA_1_DOS.

The cyberattacks between 3) and 6) refer to unauthorized access cyberattacks related to the respective IEC 60 870-5-104 commands. Similarly, the cyberattacks between 6) and 12) denote DoS cyberattacks corresponding to the IEC 60 870-5-104 commands. Fig. 1 quantifies their severity based on CVSS v3.1. It should be noted that the confidentiality requirement (CR), the integrity requirement (IR), and the availability requirement (AR) of the Environmental Group are defined to "High" since the proposed threat model is adopted in a CI so that the IEC 60 870-5-104 communications should be secured as much as possible. The other CVSS values are determined based on the nature of each IEC 60 870-5-104 command. Table II summarizes the IEC 60 870-5-104 cyberattacks, including their CVSS textual representations. Subsequently, the CVSS scores of the nonrefined nodes are propagated upper, by using the (1) and (2). In particular, (1) is applied to a parent node when it has conjunctive refinements. On the other side, (2) is used when the parent node consists of disjunctive refinements. Therefore, the CVSS scores of the refined nodes (i.e., 1) compromising confidentiality, 2) compromising integrity, and 3) compromising availability) are calculated and illustrated by Fig. 1. Moreover, the proposed threat model considers two countermeasures called "intrusion detection" and "SDN-based mitigation." The first node is responsible for the detection process, while the second undertakes to mitigate the intrusion through SDN

$$\text{CVSS}_{\text{Refined Node}} = \prod_{i=1}^{n} \text{CVSS}_{\text{Refinement}_i} \quad (1)$$

$$\text{CVSS}_{\text{Refined Node}} = \max\{(\text{CVSS}_{\text{Refinement}_1}), (\text{CVSS}_{\text{Refinement}_2}), \ldots, (\text{CVSS}_{\text{Refinement}_n})\}. \quad (2)$$

IV. Architectural Design and Intrusion Detection

The rise of the IoMT has digitized the healthcare ecosystem into a new era, known as Healthcare 4.0. The IoMT assets are deployed throughout the healthcare ecosystem, providing valuable services, such as remote and hospitalized patients' monitoring, pervasive control, and flexibility. The backbone behind such services relies on telemetry protocols, like IEC 60 870-5-104. IEC 60 870-5-104 is a telemetry protocol, which is mainly utilized in the energy sector. However, given Healthcare 4.0, hospital information system (HIS), multiple IoMT sensors, actuators, and legacy industrial healthcare systems start

TABLE II
IEC 60 870-5-104 CYBERATTACKS DESCRIPTION AND CVSS REPRESENTATION

IEC 60870-5-104 Cyberattack	Description	CVSS Representation
Man-In-the-Middle	During this attack, the cyberattacker is inserted between two endpoints, thus monitoring and controlling the network traffic exchanged.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:L/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:H/MI:L/MA:L/CR:H/IR:H/AR:H
Capturing and Dropping IEC 60870-5-104 Packets	This attack is a refinement of the Man-In-The-Middle attack, where the cyberattacker can drop the IEC 60870-5-104 packets.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:N/MA:N/CR:H/IR:H/AR:H
Traffic Sniffing	Traffic Sniffing is a passive attack, where through the MITM the cyberattacker can monitor and capture the IEC 60870-5-104 packets.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:N/MA:N/CR:H/IR:H/AR:H
C_CI_NA_1	The C_CI_NA_1 is a Counter Interrogation command in the control direction. This cyberattack sends unauthorised IEC 60870-5-104 C_CI_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_SC_NA_1	The C_SC_NA_1 command is a single command. This cyberattack sends unauthorised C_SC_NA_1 60870-5-104 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_SE_NA_1	The C_SE_NA_1 command is a set-point command with normalised values. This cyberattack sends unauthorised IEC 60870-5-104 C_SE_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_RD_NA_1	The C_RD_NA_1 command is a read command. This cyberattack sends unauthorised IEC 60870-5-104 C_RD_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_RP_NA_1	The C_RP_NA_1 command is a reset command. This cyberattack sends unauthorised IEC 60870-5-104 C_RP_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
M_SP_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 M_SP_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_CI_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_CI_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_SE_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SE_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_SC_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SC_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_RD_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_RD_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_RP_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_RP_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H

adopting IEC 60 870-5-104 to orchestrate their architectural and operational schema. In particular, IEC 60 870-5-104 comprises read and write commands like C_CI_NA_1, M_SP_NA_1 and C_RP_NA_1 that monitor or update the status of the healthcare assets. Furthermore, IEC 60 870-5-104 can handle the electrical operation of the healthcare infrastructure, monitoring and controlling the functionality of the respective substations. An IEC 60 870-5-104 cyberattack against the substation supporting the healthcare infrastructure can raise disastrous consequences or even fatal accidents. Thus, it is obvious that the interdependency between the healthcare and energy sectors is crucial, and the IEC 60 870-5-104 can affect both of them.

Fig. 2 illustrates the proposed IDPS architecture. In particular, it relies on the architectural design of the SDN technology, which consists of three main planes: 1) data plane, 2) control plane, and 3) application plane. The data plane incorporates the industrial healthcare resources, such as physical and virtual devices connected to the SDN switches. These resources are called network elements (NE). The control plane includes the SDN-C, which is responsible for orchestrating and managing the NE. To this end, the SDN-C communicates with the SDN switches through a south-bound interface (SBI). In our case, the `Ryu` controller plays the role of SDN-C, and the SBI is implemented through the OpenFlow v1.3 protocol. Finally, the application plane comprises one or more applications that can instruct the SDN-C to change the behavioral characteristics of the entire SDN network in order to serve a particular purpose, such as load balancing or cybersecurity. In this article, we use

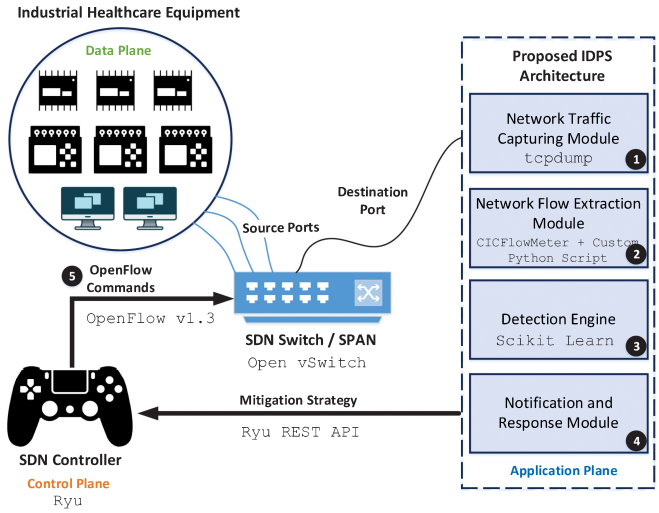


Fig. 2. Architecture of the proposed IDPS.

the SDN-C to isolate the assets related to a security event. The communication between the applications and the SDN-C is implemented through a north-bound interface (NBI). NBI is implemented via the `Ryu` REpresentational State Transfer (REST) application programming interface (API).

The proposed IDPS lies in the application plane. It consists of the following four modules:

1) network traffic capturing module (NTCM);
2) network flow extraction module (NFEM);
3) detection engine (DE);
4) notification and response module (NRM).

The NTCM monitors the SDN network and captures the IEC 60 870-5-104 network traffic through a Switched Port Analyzer. To this end, `tcpdump` is used. The NFEM receives the IEC 60 870-5-104 network traffic from the NTCM and generates the corresponding network flow statistics. In particular, two kinds of flow statistics are generated: 1) TCP/IP network flow statistics and 2) IEC 60 870-5-104 payload flow statistics. The first kind refers to bidirectional flow statistics related to the TCP/IP attributes of the IEC 60 870-5-104 packets. These statistics are generated through `CICFlowMeter`. On the other side, the second refers to bidirectional flow statistics related to the payload of the IEC 60 870-5-104 packets. To this end, a custom IEC 60 870-5-104 parser was implemented in the context of this work. Both cases are determined by a time limit, which affects the statistics and, therefore, the detection performance. This limit is defined experimentally in Section VI. The DE is responsible for the intrusion detection process based on the various statistics received from the previous module. DE integrates two complement detection models: 1) intrusion detection model (IDM) based on TCP/IP network flow statistics and 2) IDM based on IEC 60 870-5-104 payload flow statistics. Based on the evaluation analysis in Section VI, both IDMs apply a classification and regression tree (CART) classifier. CART is a decision tree composed of internal nodes and leaves that divide the overall data space into smaller subspaces based on the training features. In our case, the training features originate from the NFEM. Thus, a directed tree is created, allowing the classification of the various instances. The internal nodes represent the classification rules, while the leaves represent the classes (i.e., the IEC 60 870-5-104 cyberattacks) of the problem. The operation of the internal nodes relies on a discrete function, which divides the entire data space S into smaller subspaces $S_1, S_2, \ldots, S_k$. To this end, various criteria can be used. In our case, we apply the information gain (IG) defined by (3)–(5). $E(S_k)$ denotes the entropy of the subspace Sk, while p_i implies the probability of the i class in the subspace S_k. The entire space S is split recursively until there is no significant gain from additional separations. δ indicates the stopping criterion, regarding the splitting process. Finally, based on the detection outcome, NRM notifies the security administrator by generating the corresponding security events. In addition, NRM is responsible for deciding about the mitigation process analyzed in the following section.

If NRM takes the decision to isolate the assets related to an IEC 60 870-5-104 cyberattack, it instructs `Ryu` through the `Ryu` REST API regarding how to modify the flow tables of the SDN switch. OpenFlow is used to modify the rules in each flow table or add new rules. In our case, two rules are added. The `Ryu` REST API automates the OpenFlow commands that `Ryu` will send to the flow tables of the SDN switch. In particular, two `Ryu` REST API commands are utilized with the following fields: `dpid`, `priority`, `idle_timeout`, `hard_timeout`, `actions`, `table_id`, and `match`. The final field comprises additional subfields that identify the IEC 60 870-5-104 network flow elements, such as `in_port`, `eth_type`, `ip_proto`, `ipv4_src`, `ipv4_dst`, `tcp_src`, and `tcp_dst`. `dpid` indicates the corresponding SDN switch. `priority` denotes the priority of the specific rule. `idle_timeout` denotes the idle time before discarding. `hard_timeout` implies the maximum time before discarding. `actions` defines the instructions set of this rule, such as, for example, to drop or redirect the IEC 60 870-5-104 packets. `table_id` denotes the identifier of the table where the flow will be added. Finally, `match` indicates the criteria that will be used to map the IEC 60 870-5-104 packets with this rule. `in_port` expresses the input port of the SDN switch. `eth_type` defines the Ethernet frame type based on Internet Assigned Numbers Authority (IANA). `ip_proto` determines the protocol attribute of IPv4 based on IANA. `ipv4_src`, `ipv4_dst`, `tcp_src`, and `tcp_dst` denote the network flow elements, i.e., the source IP address, the destination IP address, the source TCP port, and the destination TCP port, respectively. The two commands are differentiated with each other based on the aforementioned network flow elements. The first command uses the `ipv4_src` and `tcp_src`, while the second command uses the `ipv4_dst` and `tcp_dst`. Both `ipv4_src` and `ipv4_dst` refer to the same IP address which is identified either as a source or destination IP address. On the other hand, `tcp_src` and `tcp_dst` equal to 2404, which corresponds to the default TCP port for IEC 60 870-5-104. Finally, regarding the installation of the proposed IDPS, the aforementioned components (i.e., NTCM, NFEM, DE, and NRM) are incorporated into a single virtual machine (VM), while SDN-C composes a different VM

$$I(S,A) = \frac{|S_1|}{|S|}E(S_1) + \frac{|S_2|}{|S|}E(S_2) + \cdots$$

$$+\frac{|S_j|}{|S|}E(S_j)=\sum_{k=1}^{k=j}\frac{|S_k|}{|S|}E(S_k) \tag{3}$$

$$E(S_k)=-\sum_{i=1}^{m}p_i\log_2(p_i) \tag{4}$$

$$\mathrm{IG}(S,A)=E(S)-I(S,A)\leq\delta. \tag{5}$$

V. SDN-Based Mitigation: Problem Formulation and Methodology

After the successful cyberattack detection, the mitigation process follows, where the NRM should decide whether the assets (i.e., physical or virtual devices) related to the IEC 6070-5-104 cyberattack will be isolated or not by the SDN-C. The continuous and proper operation of the industrial healthcare and IoMT systems using the IEC 60 870-5-104 protocol is crucial since they can monitor and control the patients' health status and the medical equipment [18]. Therefore, the NRM cannot decide arbitrarily to corrupt the potential malicious/anomalous IEC 60 870-5-104 flows since this action could lead to more devastating consequences and cascading effects. For instance, a malicious insider could perform a traffic sniffing cyberattack by a legitimate device. Based on Fig. 1, the CVSS score of this cyberattack is not very high; however, the compromised device could also be used for legitimate healthcare operations (e.g., sleep monitoring, air medical service, and medical equipment maintenance). Consequently, its isolation could result in a higher cost for the healthcare organization. On the other side, the CVSS score of those cyberattacks targeting the integrity and availability of the IEC 60 870-5-104 systems is not negligible. Despite the fact that CVSS can provide a good overview about the severity of a cyberattack, it cannot be utilized for NRM's decision since 1) it does not take into account the parameters of each environment and 2) it cannot calculate the actual cost [17].

Therefore, the response operation of NRM relies on two strategies, i.e., s_1 and s_2, denoting that NRM will instruct the SDN-C to isolate the assets related to the IEC 60 870-5-104 cyberattack or not, respectively. In the second case, the SDN-C waits for the security administrator to activate the appropriate countermeasure. Thus, each strategy is related mainly to the time when the malicious activities will be isolated. In particular, each strategy is accompanied by a particular cost. This cost implies the actual impact of the cyberattack/anomaly, and it can be measured by various values, such as monetary claims, man-hours, or, in general, unit costs. In our experiments, we adopt the third choice since we do not focus on a particular case study related to a healthcare organization. Our goal is to train the NRM in order to decide for each security event, the appropriate strategy with the best-expected reward. The expected reward called $Return$ of each strategy s_i is given by (6), where *se* and *SE* denote the corresponding and the latest security event, respectively

$$r_i(\mathrm{se})=\begin{cases}1 & \text{If the cost of } s_i \text{ is the minimum}\\ 0 & \text{Otherwise}\end{cases} \tag{6}$$

$$R_i(\mathrm{SE})=\sum_{i=1}^{\mathrm{SE}}r_i(\mathrm{se}) \tag{7}$$

$$\theta=E[R_i(\mathrm{SE})]=E\left[\sum_{i=1}^{\mathrm{SE}}r_i(se)\right]=\frac{\sum_{i=1}^{\mathrm{SE}}r_i(\mathrm{se})}{N} \tag{8}$$

$$p(\theta|R)=\frac{p(R|\theta)p(\theta)}{p(R)}\Rightarrow p(\theta|R)\propto p(R|\theta)p(\theta)$$

$$\propto\prod_{i=1}^{N}\theta^{r_i}(1-\theta)^{(1-r_i)}\left(\frac{1}{Beta(\alpha,\beta)}\theta^{a-1}(1-\theta)^{\beta-1}\right)$$

$$\propto\left(\prod_{i=1}^{N}\theta^{r_i}(1-\theta)^{1-r_i}\right)(\theta^{\alpha-1}(1-\theta)^{\beta-1})$$

$$=(\theta^{\sum_{i=1}^{N}r_i}(1-\theta)^{\sum_{i=1}^{N}1-r_i})(\theta^{\alpha-1}(1-\theta)^{\beta-1})$$

$$=(\theta^{a-1+\sum_{i=1}^{N}r_i}(1-\theta)^{\beta-1+\sum_{i=1}^{N}(1-r_i)}$$

$$\Rightarrow p(\theta|R)=Beta\left(\alpha+\sum_{i=1}^{N}r_i,\beta+N-\sum_{i=1}^{N}r_i\right) \tag{9}$$

$$\mathrm{Beta}(\alpha,\beta)=\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}\text{ where }\Gamma\text{ is the Gamma function.} \tag{10}$$

The $Return$ of each strategy s_i is defined by the random variable r_i, which follows the $Bernoulli$ distribution. Our decision problem can be transformed into a MAB problem [19], where the corresponding strategies represent the slot machines and the NRM plays the gambler's role. The goal of the gambler is to maximize the overall $Return$ (i.e., the amount of money in terms of the MAB problem). The total $Return$ and the mean $Return$ up to security event SE for each strategy s_i is given by (7) and (8), respectively. N denotes the total number where the strategy s_i is selected. To solve this kind of MAB problem, we adopt the TS method [20]. TS balances the sequential actions of an exploration–exploitation dilemma, where the $exploitation$ intends to maximize the performance, while the $exploration$ accumulates new information to improve future performance. In our problem, $exploration$ is related to investigating the $Return$ of the various NRM strategies, while $exploitation$ is related to selecting that strategy leading to the greatest mean. TS is a Bayesian-based method, which estimates the posterior $p(\theta|R)$, taking full advantage of the conjugate pairs. In Bayesian statistics, there are certain pairs of distributions, where the evidence $p(R)$ can be ignored and the posterior has the same form as the prior $p(\theta)$. These pairs are named conjugate pairs. In particular, given $R=r_1,r_2,\ldots,r_n$, the Bernoulli likelihood is equal to $p(R|\theta)=\prod_{i=1}^{N}\theta_i^r(1-\theta)^{1-r_i}, r_i\sim Bernoulli(\theta)$. Next, if we choose the prior $p(\theta)$ to follow the $Beta$ distribution (i.e., $p(\theta)=Beta(\theta;\alpha,\beta)=constant\times\theta^{a-1}(1-\theta)^{\beta-1}=\frac{1}{B(\alpha,\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1}$), then the posterior $p(\theta|R)$ follows also the $Beta$ distribution $Beta(\alpha+\sum_{i=1}^{N}r_i,\beta+N-\sum_{i=1}^{N}r_i)$, as indicated by (9), where $Beta$ is given by (10). It is noteworthy that the choice of the $Beta$ distribution is not arbitrary since in a win or lose situation where the reward is binary,

Algorithm 1: SDN-based Mitigation - TS.

```
Data: S, nPosStrategyMatrix, nNegStrategyMatrix,
      returnMatrix
Result: selectedStrategy
securityEventCounter = 0;
while True do
    Receive a security event;
    securityEventCounter = securityEventCounter +1 ;
    selectedStrategy = 0;
    maxRandom = 0;
    for strategy ← 0 to S by 1 do
        randomBeta = B(nPosStrategyMatrix[strategy]
         + 1, nNegStrategyMatrix[strategy] + 1)
        if randomBeta> maxRandom then
            maxRandom = randomBeta;
            selectedStrategy = strategy;
        end
    end
    SDN controller executes selectedStrategy;
    if
     returnMatrix[securityEventCounter][strategy]
     == 1 then
        nPosStrategyMatrix[selectedStrategy] =
         nPosStrategyMatrix[selectedStrategy +1
    end
    else
        nNegStrategyMatrix[selectedStrategy] =
         nNegStrategyMatrix[selectedStrategy +1
    end
end
```

the mean of this distribution ranges between 0 and 1. However, the output of the $Beta$ distribution ranges also between 0 and 1. Thus, for each security event, TS takes a sample drawn from the posterior probability, which equals to $Beta(\alpha = N_i^1(\text{se}) + 1, \beta = N_i^0(\text{se}) + 1)$, where $N_i^1(\text{se})$ and $\beta = N_i^0(\text{se})$ denote the number of times the strategy s_i returned 1 up to security event se and the number of times the strategy s_i returned 0 up to security event se. Algorithm 1 shows how the TS method is applied. The variables $nPosStrategyMatrix$ and $nNegStrategyMatrix$ represent $N_i^1(\text{se})$ and $N_i^0(\text{se})$, respectively.

VI. Evaluation Results

Before analyzing the experimental results, we need to present the dataset used for this purpose and the corresponding evaluation metrics. In particular, we evaluate the efficiency of the proposed IDPS in terms of 1) detection performance and 2) mitigation performance. In the first case, we created an IEC 60 870-5-104 intrusion detection dataset comprising the cyberattacks discussed in Section III. This dataset was constructed utilizing 1) seven VMs with `IEC-TestServer` representing the field devices, 2) a VM with `Qtester104` playing the role of a human–machine interface, and 3) three VMs equipped with `Metasploit`, `OpenMUC j60870`, and `Ettercap` representing the cyberattackers. Moreover, three evaluation metrics are adopted: 1) accuracy, 2) true positive rate (TPR), and 3) F1 score defined by (11)–(14), respectively. To calculate the previous evaluation metrics, the following terms are utilized. True positives (TP) denote the correct classifications concerning the malicious instances, true negatives (TN) imply the number of the correct classifications with respect to the normal instances, false negatives (FN) express the mistaken classifications regarding the malicious instances, and, finally, false positives (FP) denote the wrong classifications of the normal instances. Furthermore, we used and evaluated six flow timeouts (15, 30, 60, 90, 120, and 180ˆs) for both IDMs described in Section IV. For the flow timeouts providing the optimal detection performance, we also present a detailed ML comparative analysis, including `Logistic Regression`, `Linear Discriminant Analysis (LDA)`, `Quadratic Discriminant Analysis (QDA)`, `Decision Tree`, `Naive Bayes`, `Support Vector Machine (SVM)`, `Multilayer Perceptron (MLP)`, `Random Forest`, `Adaboost`, and two custom deep neural networks (DNNs) called `Dense DNN Relu` [21] and `Dense DNN Tanh` [21]. Finally, we compare the detection efficiency of the proposed IDPS with `Suricata`, a widely known signature/specification based IDPS. To this end, we adopt the IEC 60 870-5-104 signature rules released by `Cisco Talos`. On the other side, regarding the mitigation performance, first, we investigate how the posterior probability of $\theta|R$ ranges based on the number of the security events. To this end, we run a Python-based simulation based on the security events generated by the IEC 60 870-5-104 intrusion detection dataset created in the context of this work. The cost of each strategy for each security event was defined experimentally by security experts responsible for the cybersecurity of a healthcare center. Moreover, we compare the accuracy of the proposed solution with another relevant method called upper confident bound (UCB). The simulation and evaluation experiments were conducted on a computing system with Ubuntu 18.04.5 Long Terminal Support, Intel Core i7-6700 CPU @ 3.40 GHz 8, 16-GB random access memory and 245,1 GB solid disk drive.

Accuracy reflects the ratio between the correct classifications and the total instances. It is a fair evaluation metric when the training dataset contains an equal number of all classes

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}. \tag{11}$$

TPR denotes the portion of the original intrusion instances that were detected as intrusions

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{12}$$

False positive rate (FPR) expresses the symmetry of the normal instances that were recognized as cyberattacks

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}. \tag{13}$$

The F1 score represents the golden ratio between TPR and Precision. Precision is computed by dividing TP by the sum of TP and TN

$$F1 = \frac{2 \times \text{TP}}{2 \times \text{TP} + \text{FP} + \text{FN}}. \tag{14}$$

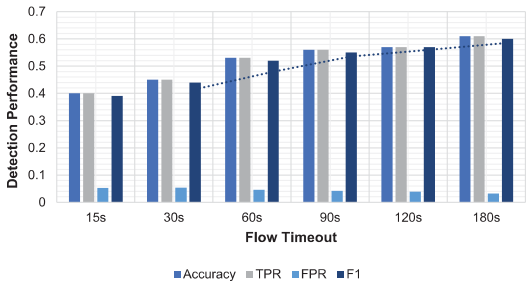


Fig. 3. IDM-TCP/IP network flow statistics.

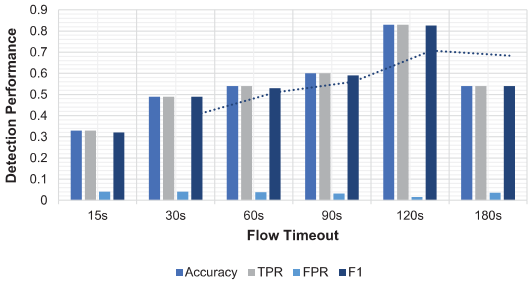


Fig. 4. IDM-IEC 60 870-5-104 payload flow statistics.

TABLE III
IDM-TCP/IP NETWORK FLOW STATISTICS—COMPARATIVE ML/DL ANALYSIS

ML Method	Accuracy	TPR	FPR	F1
Logistic Regression	0.4423	0.4423	0.0507	0.3880
LDA	0.5178	0.5178	0.0438	0.5047
QDA	0.5636	0.5636	0.0397	0.5211
Decision Tree Classifier	**0.8173**	**0.7973**	**0.0203**	**0.7921**
Naive Bayes	0.419	0.419	0.0528	0.355
SVM	0.4098	0.4098	0.0537	0.3158
MLP	0.4882	0.4882	0.0465	0.4398
Random Forest	0.5454	0.5454	0.0413	0.5283
Adaboost	0.5454	0.5454	0.0413	0.5283
Dense DNN Relu	0.5439	0.5439	0.0415	0.5198
Dense DNN Tanh	0.4995	0.4995	0.0455	0.4655
Suricata	0.6162	0.4037	0.0000	0.5752

The bold values in these tables indicate the methods with the best performance.

TABLE IV
IDM-IEC 60 870-5-104 PAYLOAD FLOW STATISTICS—COMPARATIVE ML/DL ANALYSIS

ML Method	Accuracy	TPR	FPR	F1
Logistic Regression	0.6223	0.6223	0.0343	0.6053
LDA	0.6183	0.6183	0.0347	0.6055
QDA	0.6085	0.6085	0.0356	0.5340
Decision Tree Classifier	**0.8314**	**0.8314**	**0.0153**	**0.8258**
Naive Bayes	0.5582	0.5582	0.0402	0.4749
SVM	0.5537	0.5537	0.0406	0.4805
MLP	0.5902	0.5902	0.0373	0.5702
Random Forest	0.6647	0.6647	0.0305	0.6473
Adaboost	0.2500	0.2500	0.0682	0.1818
Dense DNN Relu	0.6425	0.6425	0.0325	0.5988
Dense DNN Tanh	0.5769	0.5769	0.0385	0.0385
Suricata	0.6162	0.4037	0.0000	0.5752

The bold values in these tables indicate the methods with the best performance.

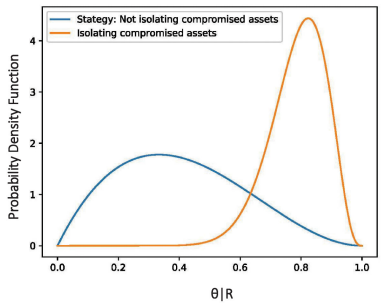


Fig. 5. Strategy probability density function after 20 security events.

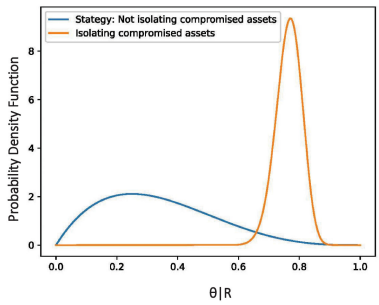


Fig. 6. Strategy probability density function after 100 security events.

Figs. 3 and 4 depict the detection performance for the IDMs using 1) TCP/IP network flow statistics and 2) IEC 60 870-5-104 payload flow statistics, respectively. In the first case, the best detection performance is achieved when the flow timeout equals 180 s. In contrast, when the IEC 60 870-5-104 payload flow statistics are used, the optimal detection performance is achieved when the flow timeout is equal to 120 s. In both cases, the numerical results rely on the CART decision tree. In particular, Tables III and IV present the comparative ML analysis for each case. When the TCP/IP network flow statistics are used, the best detection performance is achieved by the CART decision tree, where Accuracy $= 0.8173$, TPR $= 0.7973$, FPR $= 0.0203$, and $F1 = 0.7921$. The worst performance is achieved by SVM, where Accuracy $= 0.4098$, TPR $= 0.4098$, FPR $= 0.0537$, and $F1 = 0.3158$. Similarly, when the IEC 60 870-5-104 payload flow statistics are utilized, the CART decision tree also achieves the maximum detection performance, where Accuracy $= 0.8173$, TPR $= 0.7973$, FPR $= 0.0203$, and $F1 = 0.7921$. In this case, the minimum efficiency is accomplished by Adaboost, where Accuracy $= 0.2500$, TPR $= 0.2500$, FPR $= 0.0682$, and $F1 = 0.1818$.

Regarding the mitigation performance, Figs. 5–8 illustrate how the posterior probability defined in Section V ranges based on the number of 20, 100, 200, and 2000 security events for each strategy. We can see that the probability density function is made skinnier and taller as more security events are generated by the proposed IDPS, thus increasing our belief for each strategy. Finally, Fig. 9 compares the accuracy of the TS method with a relevant UCB method with respect to 5, 10, 20, 50, 100, 200, 1000, 1500, and 2000 security events. In contrast with TS, UCB does not use samples from the posterior probability, but it relies on a predefined threshold. The mitigation accuracy of TS reaches 0.932. We can also observe that the proposed TS

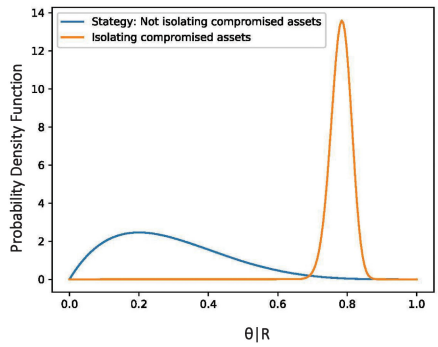


Fig. 7. Strategy probability density function after 200 security events.

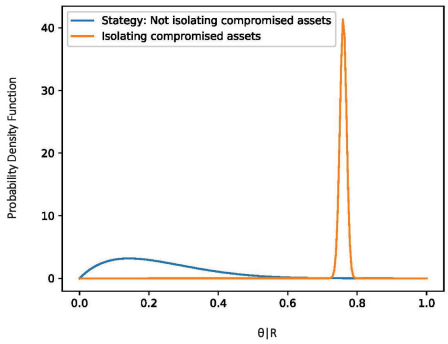


Fig. 8. Strategy probability density function after 2000 security events.

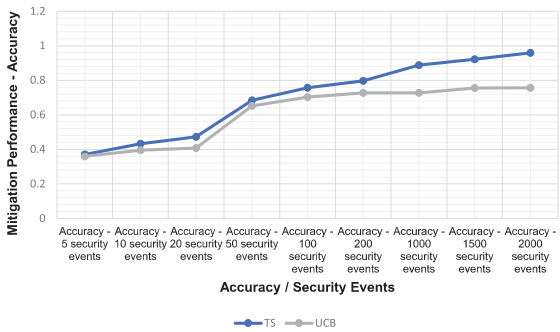


Fig. 9. Accuracy comparison between the proposed TS method and UCB.

method exceeds the UCB efficiency for each number of security events.

VII. Conclusion

Despite the necessary digitization of the healthcare ecosystem, the IoMT progression and mainly the insecure nature of the legacy healthcare systems increase 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 cyberattacks 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 cyberattacks. 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 cyberattacks related to IEC 60 870-5-104 and other industrial and IoMT protocols utilized in the healthcare sector, such as Modbus, MQTT, and EtherCAT. To this end, ML-based association rules techniques will be adopted.

Acknowledgment

This article is dedicated to the memory of Nikolaos Panagiotarakis (Project Officer of SDN-microSENSE) who passed away during the preparation of this work.

References

[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, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA systems," 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.

[11] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based wbans," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020.

[12] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[13] S. Meng *et al.*, "Security-aware dynamic scheduling for real-time optimization in cloud-based industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4219–4228, Jun. 2021.

[14] H. Lin, "SDN-based in-network honeypot: Preemptively disrupt and mislead attacks in IoT networks," 2019, *arXiv:1905.13254*.

[15] T. Xing, Z. Xiong, D. Huang, and D. Medhi, "SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds," in *Proc. 10th Int. Conf. Netw. Serv. Manage. Workshop*, 2014, pp. 308–311.

[16] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Attack-defense trees," *J. Log. Comput.*, vol. 24, no. 1, pp. 55–87, 2014.

[17] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke, "Can the common vulnerability scoring system be trusted? A Bayesian analysis," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1002–1015, Nov./Dec. 2018.

[18] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.

[19] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, "Achieving resilience in SDN-based smart grid: A multi-armed bandit approach," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops*, 2018, pp. 366–371.

[20] D. Russo, B. Van Roy, A. Kazerouni, I. Osband, and Z. Wen, "A tutorial on thompson sampling," 2017, *arXiv:1707.02038*.

[21] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, and E. Panaousis, "Aries: A novel multivariate intrusion detection system for smart grid," *Sensors*, vol. 20, no. 18, 2020, Art. no. 5305.

Panagiotis Radoglou-Grammatikis (Member, IEEE) received the M.Eng. degree in informatics and telecommunications engineering in 2016 from the Department of Informatics and Telecommunications Engineering (now Department of Electrical and Computer Engineering), Faculty of Engineering, University of Western Macedonia, Kozani, Greece, where he is currently working toward the Ph.D. degree.

He is currently a Research Associate with the University of Western Macedonia, Kozani, Greece, in national- and European-funded research projects, including SPEAR, MARS, SDN-microSENSE, TERMINET, and EVIDENT. He possesses working experience as a Security Engineer and Software Developer. He has authored or coauthored more than 20 research papers in international scientific journals, conferences, and book chapters. His main research interests are in the area of cybersecurity and mainly focus on intrusion detection, vulnerability research, and applied cryptography.

Mr. Radoglou-Grammatikis was a Reviewer for several scientific journals. He is a member of the Technical Chamber of Greece.

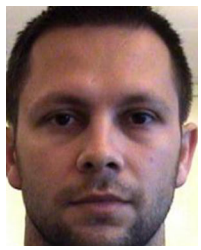
Konstantinos Rompolos received the M.Eng. degree in informatics and telecommunications engineering from the Department of Informatics and Telecommunications Engineering (now Department of Electrical and Computer Engineering), Faculty of Engineering, University of Western Macedonia, Kozani, Greece, in 2020.

He was a Researcher with the ARRANGE-ICT, an Erasmus+ research project, cofunded by the European Union. He has authored or coauthored two research papers in international conferences.

Panagiotis Sarigiannidis (Member, IEEE) received the B.Sc. and Ph.D. degrees from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively, both in in computer science.

He is the Director of the ITHACA lab, Kozani, Greece and an Associate Professor with the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani, Greece. He has authored or coauthored more than 200 papers in international journals, conferences, and book chapters. He has been involved in several national, European, and international projects. He is currently the Project Coordinator of three H2020 projects, namely SPEAR, EVIDENT, and TERMINET. He also coordinates the Operational Program MARS and the Erasmus+ KA2 ARRANGE-ICT: SmartROOT. He also serves as a Principal Investigator with H2020 SDN-microSENSE, and with three Erasmus+ KA2: ARRANGE-ICT, JAUNTY, and STRONG. His research interests include telecommunication networks, Internet of Things, and network security.

Dr. Sarigiannidis participates on the Editorial Boards of various journals.



Vasileios Argyriou received the B.Sc. degree in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and the M.Sc. and Ph.D. degrees from the University of Surrey, Guildford, U.K., in 2003 and 2006, respectively, both in electrical engineering working on registration.

From 2001 to 2002, he held a research position at the AIIA Lab, Aristotle University, working on image and video watermarking. In 2007, he joined the Communications and Signal Processing (CSP) Department, Imperial College, London, U.K., where he was a Research Fellow working on 3-D object reconstruction. He is currently a Professor with Kingston University, Kingston, U.K., working on computer vision and artificial intelligence for crowd and human behavior analysis, computer games, entertainment, and medical applications. His research interests include educational games and human-computer interaction for augmented and virtual reality systems.

Thomas Lagkas received the Ph.D. in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2006.

He is currently an Assistant Professor with the Department of Computer Science, International Hellenic University, Thermi, Greece. From 2012 to 2019, he was a Lecturer and then a Senior Lecturer with CITY College, International Faculty, The University of Sheffield, Sheffield, U.K.. He was the Research Director with the Computer Science Department, CITY College, and the leader of the ICT Track of the South-East European Research Centre. He has authored or coauthored more than 90 publications in widely recognized international scientific journals and conferences. His research interests are in the broad area of Internet of Things communications.

Dr. Lagkas is a Fellow of the Higher Education Academy, Heslington, U.K. He also participates in the Editorial Boards of respectful scientific journals and is actively involved in drafting research funding proposals as well as in the implementation of the corresponding EU projects.

Antonios Sarigiannidis received the B.Sc. degree in information technology, the M.Sc. degree in communication systems and technologies, specializing in advanced optical and wireless technologies, and the Ph.D. degree in information technology from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2007, 2009, and 2016, respectively.

His Ph.D. thesis includes the development of bandwidth allocation algorithms in communication networks. Recently, he has been involved in Internet of Things and machine to machine research toward coverage analysis and security services. He actively participated in both national- and EU-funded projects. He is the author of more than 30 publications in leading international journals and conferences. His research interests include machine learning mechanism and optimization techniques as well as visualization techniques regarding analytics, big data, and security analysis.

Sotirios K. Goudos (Senior Member, IEEE) received the B.Sc. degree in physics, the M.Sc. of Postgraduate Studies in electronics, and the Ph.D. degree in physics from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1991, 1994, and, 2001, respectively, the M.Sc. degree in information systems from the University of Macedonia, Thessaloniki, Greece, in 2005, and the diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki in 2011.

He is currently an Associate Professor with the Department of Physics, Aristotle University of Thessaloniki. He is the Director of the ELEDIA@AUTH lab. His research interests include antenna and microwave structures design, evolutionary algorithms, wireless communications, machine learning, and semantic web technologies.

Dr. Goudos has participated as Guest Editor or Lead Guest editor for more than 20 special issues in international journals. He is a member of the ELEDIA Research Center Network.

Shaohua Wan (Senior Member, IEEE) received the Ph.D. degree in edge intelligence from the School of Computer, Wuhan University, Wuhan, China, in 2010.

Since 2015, he has been holding a Postdoctoral position with the State Key Laboratory of Digital Manufacturing Equipment and Technology, Huazhong University of Science and Technology, Wuhan. From 2016 to 2017, he was a Visiting Professor with the Department of Electrical and Computer Engineering, Technical University of Munich, Munich, Germany. He is currently an Associate Professor with the School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan. He is an Author of more than 130 peer-reviewed research papers and books, including more than 30 IEEE/ACM Transactions papers such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *ACM Transactions on Internet Technology*, IEEE TRANSACTIONS ON MULTIMEDIA, *ACM Transactions on Multimedia Computing, Communications, and Applications*, PR, etc. and many top conference papers in the fields of multimedia. His main research interests include deep learning for Internet of Things and edge computing.