Modeling, Detecting, and Mitigating Threats

Against Industrial Healthcare Systems: A

Combined Software Defined Networking and

Reinforcement Learning Approach

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 cyberattacks by providing a quantitative threat model, which relies on Attack Defence Trees and CommonVulnerability 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.

**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], 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 Alien- Vault OSSIM risk model.

Hodo *et al.* [3] adopt variousMLalgorithms 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.

**Disadvantages**

* The system is not implemented SDN-BASED MITIGATION: PROBLEM FORMULATION AND METHODOLOGY.
* The system is not implemented enough method for testing and training for large datasets.

Proposed System

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].

**Advantages**

* The proposed system implemented 1) detection performance and 2) mitigation performance which are enough operations on datasets.
* The proposed system developed notification and response module (NRM) for datasets prediction.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 7 Ultimate.
* **Coding Language :** Python.
* **Front-End :** Python.
* **Back-End :** Django-ORM
* **Designing :** Html, css, javascript.
* **Data Base :** MySQL (WAMP Server).