Securing connection between IT and OT: the Fog Intrusion Detection System prospective

Riccardo Colelli
Department of Engineering
University of Roma Tre
Rome, Italy
riccardo.colelli@uniroma3.it

Stefano Panzieri
Department of Engineering
University of Roma Tre
Rome, Italy
stefano.panzieri@uniroma3.it

Federica Pascucci
Department of Engineering
University of Roma Tre
Rome, Italy
federica.pascucci@uniroma3.it

***Abstract*—Industrial Control systems traditionally achieved security by using proprietary protocols to communicate in an isolated environment from the outside. This paradigm is changed with the advent of the Industrial Internet of Things that foresees flexible and interconnected systems. In this contribution, a device acting as a connection between the operational technology network and information technology network is proposed. The device is an intrusion detection system related to legacy systems that is able to collect and reporting data to and from industrial IoT devices. It is based on the common signature based intrusion detection system developed in the information technology domain, however, to cope with the constraints of the operation technology domain, it exploits anomaly based features. Specifically, it is able to analyze the traffic on the network at application layer by mean of deep packet inspection, parsing the information carried by the proprietary protocols. At a later stage, it collect and aggregate data from and to IoT domain. A simple set up is considered to prove the effectiveness of the approach.**

***Index Terms*—Cybersecurity, Intrusion Detection System, Industrial Internet of Things, Fog Computing, New Implementation Approaches, Industrial Informatics.**

I. Introduction

Industrial control systems has been created inside isolated environments, for this reason protection from the outside threats was always guaranteed to them. Today, with the advent of Internet of Things (IoT) and the need to be able to communicate different devices among themselves in the industrial plant (Industrial IoT), Operational Technology (OT) systems are more vulnerable to new types of threats. An Industrial Control System Architecture could be divided in different physical and digital layer depending on the control [10]:

- Layer 0: Fieldbus and operative part include the action chains and the acquisition chains. The action chain is responsible for achieving the transformation into the production flow (i.e., actuators). The acquisition chain is involved in monitoring the product flow evolution (i.e., sensors);
- Layer 1: Local control defines process evolution by the control law. Digital embedded devices control such as Programmable Logic Controllers (PLCs) are responsible for the sequential control;
- Layer 2: Supervisory control And Data Acquisition (SCADA) systems store process data and alarm status. Through a Human Machine Interface (HMI) the operator is able to regulate the control law or to manage anomalies.

SCADA systems are used to remotely monitor industrial controls and ensure the proper functioning of processes involving critical plants or critical infrastructures. In the latter case, infrastructure control is a key of importance for the country (e.g. power grid) and therefore, a failure of these could cause extensive damage. Consequently, it is important protect these systems from all kind of threats, including cyber threats.

In recent years, OT systems have been targeted by different cyber threats. Stuxnet [2] is a worm that utilizes at least some vulnerabilities of Microsoft operating system, including zero-day vulnerabilities. Stuxnet had to disable the centrifuges of the power plant in Natanz, preventing the detection of malfunctions induced by Stuxnet itself. The power grid attack against Ukraine [8] is one of the most recent case relating to cyber attack in OT. This cyber attack is considered the first one against power grid and it caused substantial losses to the target country. Nowadays, the IIoT could be considered the result of the convergence between Information Technology (IT) and Operational Technology. Big Data, Horizontal and vertical connection between the devices in the plant and, finally, the connection to the cloud, open up the way to new cyber threats in the industrial environment. Regarding IT, many strategies about cyber security have been implemented over time, however cyber security in OT must be handled differently. Indeed, wanting to draw a ranking of priorities in OT, Availability plays a key role, followed by Integrity and then Confidentiality (AIC) [15]; in IT the priorities are in the reverse order (i.e., CIA). According to this, until the industry 4.0, the availability of data reaches levels of extreme importance at the expense of confidence, i.e., an non encrypted data has always been preferred as long as it is transmitted in real-time. Another aspect that strongly distinguishes OT from IT is the presence of cyber physical systems in the OT. Therefore, an appropriate control through the network is performed at the same time to a fault monitoring. Using process modeling tools and by monitoring the process a fault could be distinguished from a cyber attack. In this paper, a tool that connects the legacy part of the industrial control system and the IT level is proposed, in order to securing the controls of the cyber physical systems

978-1-7281-0429-4/19/$31.00 ©2019 IEEE

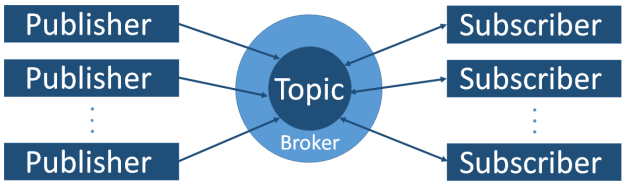


Fig. 1: MQTT publish/subscribe

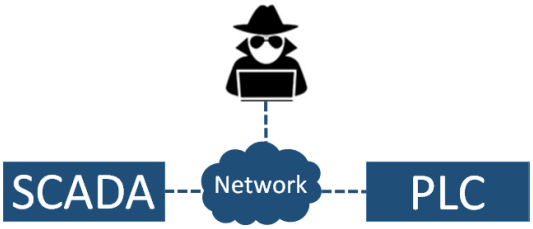


Fig. 2: Attack scanario

and e provide data to the IoT devices. An approach that can be exported from the IT networks in order to securing the traffic is the Intrusion Detection System (IDS), whereby it is possible monitoring data exchange over the network and identifying possible threats. Snort [18] is the most popular open-source packets sniffer, it is able to detect a huge set of attacks through the definition of rules. Another signature based IDS is Suricata [19]. In this paper an IDS for OT domain is presented: the first contribution is related to the features analyzed to identify threats and the second contribution is referred to the IIoT communication. More specifically, the proposed tool connects securely devices from the industry (PLC, SCADA) with devices comply with the founding technologies of the Internet of Things but external to the process of the plant. Using deep packet inspection applied to the specific protocol the proposed IDS is able to identify anomalies in the monitored process. Thus, the probe of the IDS is implemented using Scapy [16] in order to analyze the traffic in the network. This tool is implemented considering all the components that are part of an IDS: event generator, event analyzers, response units and event databases [7]. Furthermore, a communication layer is created in order to report data passing through the IDS with the Message Queue Telemetry Transport (MQTT) protocol [14]. MQTT is a messaging protocol introduced in 1999 by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom and was standardized in 2013. MQTT connect embedded device and network applications, for this reason it is particularly suitable for the Internet of Things. In particular, the connection could be one-to-one, one-to-many and many-to-many [1] and it allows also horizontal communication between smart devices. MQTT utilizes a proper pattern named publish/subscribe to provide easiness and flexibility as shown in Fig. 1. In particular, a client sends a message (publisher) to the other client (subscriber). The connection is provided by a third component (broker) that filters the incoming message depending on the topic. Considering that MQTT is suitable for resource constrained devices and it is build over the TCP protocol layer, it is indicated for embedded systems or smart sensor that are included in the smart factory. MQTT delivers messages using three Quality of Service (QoS) levels. QoS level 0 is the delivery at most once: the messages is delivered based on the effort of the network. QoS level 1 is one delivery at least once: the message is being sent at least once and the duplicate may exist in messages. QoS level 2 is called exactly once: guarantee that the message is delivered only once [21]. Furthermore, it is possible increasing safety about MQTT through tasks that make the publish/subscribe pattern safe [17]. It is apparent that IDS positioned in the monitoring port of the switch, in nominal condition, has the role of centralizing the legacy systems similar to the fog element [5]. Thus, the Fog Intrusion Detection System (FIDS) preserves the ability to identify a cyber attack and provides the IT, in a safe way, data on the status of the process. On the other hand, measurement coming from IoT sensor increase the chance of detecting the attack. The industrial protocol considered in this work is a device-independent and fieldbus-independent interface the Automation Device Specification (ADS), used in TwinCAT Beckhoff Systems [3]. Although Scapy is able to decode packets of many protocols, however, it does not provide support for ADS, to this end a specific parser has been also developed.

II. Proposed Approach

The protection strategy of data exchange between SCADA and devices devoted to real-time control is proposed in this contribution. Specifically, the Industrial Control System scenario foresees by IIoT paradigm is investigated. As shown in Fig. 2, two main actors have been considered, in the first phase of the approach: a PLC and a SCADA system. The values of sensors and actuators on the operative side are directly connected with the registers in the PLC. SCADA system receives the information from PLC in order to monitor the process and provide the operator with a graphical interface. The PLC and the SCADA system are connected by network services, that bring weaknesses and vulnerabilities. Cyber attacks on the communication channel are investigated: to this end, an attacker is supposed able to gain access to the network so to discover the weaknesses of the controlled process. To protect the communication channel, an IDS both signature and anomaly based is developed. The IDS signature based behaves like an anti-virus software: rules are previously established and a violation of them produces an alert. The IDS uses the signature to analyze the packets over the network in order to detect the specific threats of IT domain. If an attack does not violate any rules, this kind of IDS is not effective, since rules are established according to known attacks. The proposed IDS is able to parser the packet of industrial protocol using deep packet inspection approach. Thus, the sequence of commands, inside the payload, are analyzed to overcome the limits of the signature based. Moreover, the IDS knows the nominal behavior of the system and is able to detect

deviations and it can detect new threats. To collect alerts, the IDS exploits a database and it feeds three different tables. The first table stores attacks on network protocol TCP/IP, e.g. denial of service, port scan, man-in-the-middle using the signature approach. The second one, through the payload analysis, collects commands that are exchanged between the devices and redirected by the monitoring port to IDS. Finally, the third table is used by the intrusion detection engine for the analysis on the behaviour of the system, in according with values in the second table. The topology network based is able to cope with legacy system without being invasive and to process data to and from IoT at the same time.

A. IDS network based

The implementation of the proposed IDS relies on mirroring strategy implemented on most of the commercial routers and switches. Thus, the IDS device is connected to the monitoring port and the traffic of the whole network is analyzed. IDS has been implemented using the Industrial PC C6015 produced by Beckhoff, an ultra-compact industrial PC. For implemented the IDS network based, a Unix operating system is used, even though the physical device produced by Beckhoff is provided with a Windows Operating System. The decision of changing the operating systems is derived from the flexibility of this tool. In Linux environments packet filtering and blocking are available by programming firewall rules. In fact, the Linux kernel firewall provides the use of Iptables. In particular, in this paper, Iptables are used to block packets coming from IoT to legacy devices. Network segmentation is compliant with the Defense-in-Depth Architecture in cyber-physical system [11]. Network segmentation creates different networks from the original one, in order to limit possible damage to each zone. Moreover, a firewall between manufacturing zone and the non-real time zone (e.g., IoT) establishes an Industrial Demilitarized Zone that avoids direct communications between the two zones.

The IDS is implemented exploiting the packet manipulation tool Scapy. Written in Python and Based on Nmap, Scapy is able to analyze traffic on the network and send packets to the other devices. It analyzes all the traffic between the SCADA system and the PLC. The IDS aims to identify possible malicious attack over the network and it contains inside the three tables previously described. In this approach, MySQL is used to implement the IDS database. Whenever IDS identifies an intrusion, it communicates promptly to the operator in the control room. IDS allows to view attacks from the network level that are reported in the first table (e.g., Port Scan and ARP poisoning aimed to eavesdropping). Furthermore, this tool has a field for viewing the variables monitored, in this way there is a redundancy with the main HMI in the SCADA in order to guarantee the robustness of the system under attack. Concerning the third table, it contains notification of a variable with a value not considered as normal. To build this table, a Python script able to parser the ADS protocol by Beckhoff TwinCAT has been developed. Lastly, the anomaly based script runs together with the IDS analyzer and compares values

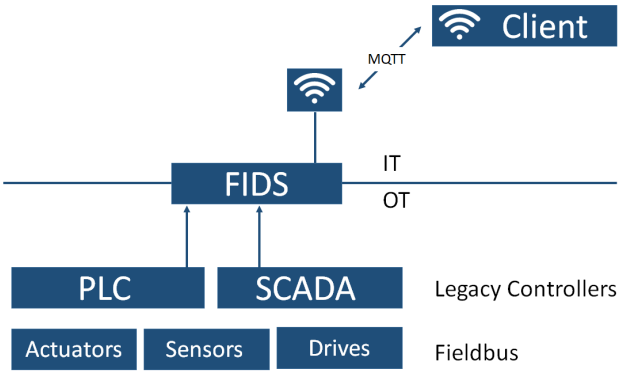


Fig. 3: Architecture of Fog Intrusion Detection Systems

from the second tables with the nominal behaviour, thereby a notification of intrusion is generated.

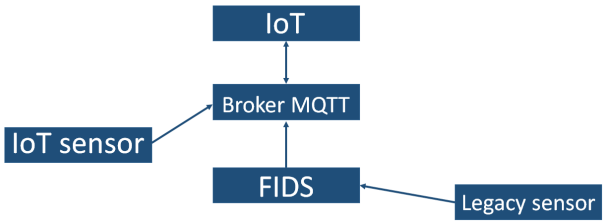
B. MQTT communication

It is possible dedicate one outo of the two network interfaces of the C6015 device to the MQTT communication, in particular for devices outside the process plant as shown in Fig. 3. For the sake of simplicity, in this paper, Legacy Controllers is referred to both type of control. Through a wireless router, MQTT traffic is generated by the C6015, in this way information about the legacy devices could be published over a specific topic. Clients receive the comprehensive data through the topic in MQTT. In this regard devices as smart sensor for monitoring the plant or devices used by the operators are inserted. Furthermore, through the MQTT protocol the device is able to report OT network anomalies to the Security Operation Center (SOC). As mentioned before, there is a complete separation from the two operative layers with regard to control to be implemented in the field. Thus, for security reason, strict rules are implemented in the Linux firewall over C6015 in order to deny any link between the two subnetworks. Thereby, treats coming from IT (e.g., man-in-the-middle) cannot influence the legacy components involved in the control. The tool under discussion allows an overview of the process layer, as a data collector (i.e., fog computing function), at once it prevents the compromise of process. Firewall, which is a main way to prevent network attacks, is often used to prevent illegal connection and divides the internal networks from insecure actions. MQTT protocol could be readily implemented inside smart component such as ESP8266 nodeMCU [12], shown in Fig. 6. Its feature are shown in TABLE I.

C. Redundancy strategy

Devices from IoT may facilitate the identification of faults resulting from physical failures and/or cyber attacks. For this purpose, it is necessary to duplicate the measurement coming from the monitored process. In [13], the relationship between redundancy and security is analyzed. Moreover, in terms of independence of the measurements, it is necessary a proper separation against faults affecting the components. In the

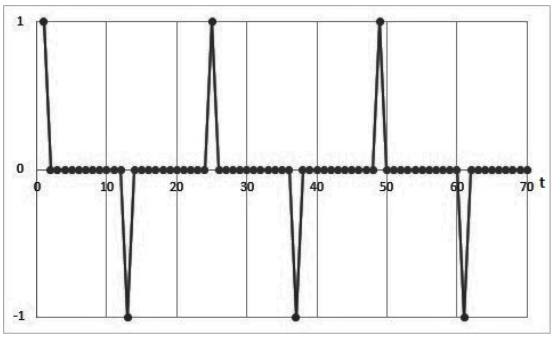
event of an industrial network assisted by an IoT network layer, the IDS proposed provides a proper separation of the events. Redundancy could use in SCADA environment in order to detect false information related to cyber attacks [20]. The redundant components are fault-tolerant with the proper diversity in order to avoid a signle-point of failure [4]. The possible configuration are shown in Fig. 4.



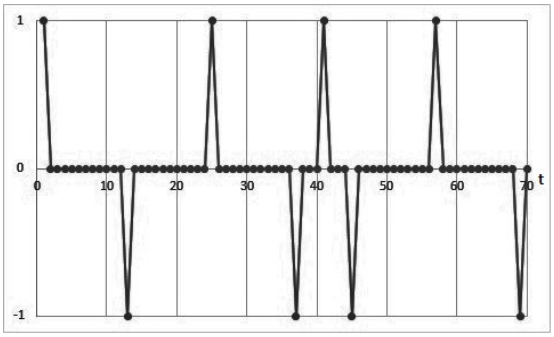
(a) IoT compliant

(b) Redundancy

Fig. 4: Fog intrusion detection system configuration



(a) Normal behaviour



(b) Disrupted behaviour

Fig. 5: False data injection effect

III. Results

To prove the effectiveness of the IDS approach, the proposed anomaly based IDS has been tested and was investigated in [6]. The intrusion detection system is implemented over a Beckhoff C6015 Industrial PC. This industrial device is equipped with two network interfaces used, in this paper, for connect legacy systems with IoT. In this framework, the PLC CX2030 represent the real-time device and it communicates with the SCADA system according to the Automation Device Specification (ADS) protocol. The ADS developed within the TwinCAT architecture communicate exploiting TCP/IP stack as transport layer. Real-time device and SCADA are connected by means of a switch to the network. The embedded PC is connected to a virtual system, that emulates a simple Automated Guided Vehicle (AGV) in a Visual Studio .NET framework. The AGV is moving on a straight path between two target points. When the AGV reaches a limit, it stops and go back to the other one. An attacker is connected to the local area network switch. To test the proposed system, two different attacks are proposed by the malicious actor. During the first attack, the transportation layer is targeted through an ARP poisoning by using the Kali Linux tool named Ettercap. In this eavesdropping attack, data are captured on the network by associating MAC address of the attacker with the IP address of the target. The signature based IDS analyzer is able to detect the ARP poisoning by comparing the MAC address with the corresponding IP address inside a white list. This solution is effective on the industrial network, since the topology is more static in OT (e.g., legacy systems) then in IT domain. The second attack targets the application layer. The attacker performs a two stages attack. At the beginning, he/she only knows the machines to be targeted and eavesdrops the data exchanged. By parsing the protocol, the attacker is able to form a rough idea on the system attacked (i.e., the expected values, the nominal behavior, etc) and tries to perform a more complex attack by modifying the data in the payload in order to disrupting the process. In the IDS, a parser for ADS has been implemented to deeply inspect the packets and analyze them at application layer. A proper parser has been implemented since Scapy cannot parse ADS protocol. The anomaly based strategy grabs the control variables and store the value in the second table (i.e., the sensor output). By comparing the nominal operating mode with respect to the actual one, it is possible to detect anomalies. In Fig. 5 the mismatch between the nominal and the anomalous behaviour is shown. The peaks represent respectively the left and the right limit during the time. Under normal operating conditions, the AGV reaches the targets point regularly. When the system is attacked, the signals are faked: specifically, the AGV seems to reach a target point, so the control algorithm send it back to the other one. The IDS detects the mismatch behavior and set an alarm in the alert table. To prove the IDS compatibility with the IoT environment, a nodeMCU platform is used. In order to ensure the communication from the C6015 and the IoT platform, a broker MQTT is installed over the IDS. In particular, Eclipse Mosquitto [9] is implemented as a broker. Furthermore, the experimental result aim to demonstrate the redundancy strategy. For this purpose, nodeMCU platform communicate through MQTT protocol to the IDS the redundant measurement (i.e., end of AGV path). NodeMCU publishes the value through a

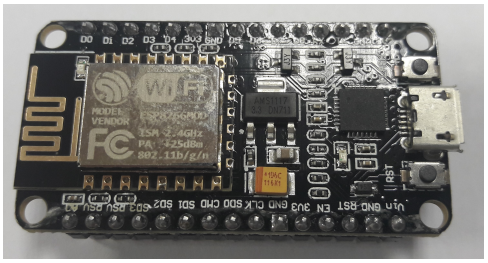


Fig. 6: ESP8266 nodeMCU

wireless Local Area Network created specifically by a router, which is linked to a Network Interface of the C6015 by wire. Detection strategy is assisted by the redundant measure coming from the IoT channel. Thereby, the attacker should be able to simultaneously attack the two channels to avoid being discovered, considering that legacy OT network and IoT network are properly divided by the Linux firewall.

TABLE I: Features of nodeMCU

Component	Specification
Flash memory	4MB
Scripting language	2 buttons
GPIO pins	17 GPIO
ADC	1 - 10 bit
Operation modes	Station / SoftAP / SoftAP+station
Operating voltage	3.3 V
Wireless Standard	802.11 b/g/n
Programmer	USB-UART CP2102
module	ESP-12E

IV. Conclusion

In this contribution, an IDS for industrial control system is presented as a device that bring together data from the OT network. To this aim, a MQTT client is implemented in the IDS implemented in a Beckhoff C6015. Data from fieldbus can be safely analyzed by smart devices that are connected in the Industrial IoT network such as smart sensor for monitoring the plant or devices used by the operators for process control of the plant. The detection function of the IDS is maintained, in particular a specific parser for industrial protocols is developed and a baseline for the nominal behavior of the plant is formed. The proposed approach has been implemented over Beckhoff CX2030 and a SCADA system, controlling the motion of a virtual AGV. The obtained results are encouraged, since the IDS does not introduce significant delay in the system and it is able to improve the awareness of the system. Although the results are promising, there is still room for improvements. The IDS is supposed inside the operating domain: in an industrial set up, indeed, the firewall protect the perimeter, so the IDS analyzes all the packets that have passed the firewall. A more efficient approach would be obtained by inserting in the network two IDSs, one before and the other one after the firewall, to get insights on how an attack starts and where a threat comes from. The Database is designed to be flexible: the tables that are filled by the IDS can be local or remote. This allows to implement the Database either in a local machine or directly in the cloud trough MQTT communication. In future development more complex approach can be adopted by exploiting the model of the plant. In this way, the IDS would be able to detect faults and attacks, improving the maintenance schedule of the system.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.

[2] Antiy Labs. Report on the worm stuxnets attack, October 2010.

[3] Beckhoff. https: //infosys.beckhoff.com/ Accessed: 2018-05-08.

[4] A. A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500, June 2008.

[5] M. Chiang and T. Zhang. Fog and iot: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6):854–864, Dec 2016.

[6] R. Colelli, S. Panzieri, and F. Pascucci. Exploiting system model for securing cps: the anomaly based ids perspective. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 1171–1174, Sep. 2018.

[7] Igino Corona, Giorgio Giacinto, and Fabio Roli. Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. *Information Sciences*, 239:201 – 225, 2013.

[8] E-ISAC. Analysis of the cyber attack on the ukrainian power grid, March 2016.

[9] Eclipse Mosquitto. https ://mosquitto.org/ Accessed: 2018-05-08.

[10] C. Escudero, F. Sicard, and E. Zamai. Process-aware model based idss for industrial control systems cybersecurity: Approaches, limits and further research. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 605–612, Sep. 2018.

[11] N. Jiang, H. Lin, Z. Yin, and C. Xi. Research of paired industrial firewalls in defense-in-depth architecture of integrated manufacturing or production system. In *2017 IEEE International Conference on Information and Automation (ICIA)*, pages 523–526, July 2017.

[12] R. K. Kodali and B. S. Sarjerao. A low cost smart irrigation system using mqtt protocol. In *2017 IEEE Region 10 Symposium (TENSYMP)*, pages 1–5, July 2017.

[13] Bev Littlewood and Lorenzo Strigini. Redundancy and diversity in security. In Pierangela Samarati, Peter Ryan, Dieter Gollmann, and Refik Molva, editors, *Computer Security – ESORICS 2004*, pages 423–438, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[14] Dave Locke. Mq telemetry transport (mqtt) v3. 1 protocol specification. *IBM developerWorks Technical Library*, page 15, 2010.

[15] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J. Cruz. Cyber security of critical infrastructures. *ICT Express*, 4(1):42 – 45, 2018. SI: CI Smart Grid Cyber Security.

[16] Scapy. https: //scapy.net/ Accessed: 2018-05-08.

[17] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar. Secure mqtt for internet of things (iot). In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pages 746–751, April 2015.

[18] Snort. https: // snort.org/ Accessed: 2018-05-08.

[19] Suricata. https: //suricata-ids.org/ Accessed: 2018-05-08.

[20] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry. Cyber security analysis of state estimators in electric power systems. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5991–5998, Dec 2010.

[21] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi. Internet of things: Survey and open issues of mqtt protocol. In *2017 International Conference on Engineering MIS (ICEMIS)*, pages 1–6, May 2017.