Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol

WORD COUNT	5136	TIME SUBMITTED	19-JUL-2021 01:50PM
		PAPER ID	74638584

Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol

[1st] M. Agus Syamsul Arifin
Faculty of Computer Universitas Bina Insan/Faculty of Engeenering Universitas Sriwijaya
Lubuklinggau, Indonesia
mas.arifin@univbinainsan.ac.id

[2nd] Deris Stiawan*
Faculty of Computer Science Universitas Sriwijaya
Palembang, Indonesia
deris@unsri.ac.id

[3rd] Susanto
Faculty of Computer Universitas Bina Insan/Faculty of Engeenering Universitas Sriwijaya
Lubuklinggau, Indonesia
susanto@univbinainsan.ac.id

[4th] Dwi Prasetya
Manager of Operation Facility PLN, UP2D S2JB
Palembang, Indonesia
dwi.prasetya@pln.co.id

[5th] Mohd. Yazid Idris
faculty of Computer Science and Information System,Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
yazid@cs.utm.my

[6th] Rahmat Budiarto
College of Computer Science and IT, AlBaha University
Albaha, Saudi Arabia
rahmat@bu.edu.sa

***Abstract*— As SCADA (Supervisory Control Acquisition Data) has extended to a heterogeneous network, makes it opens to any types of internet attack/malicious activity. Malicious activities in the SCADA network may disrupt the control and monitoring process of industrial equipment. These activities can be in the form of Unauthorized Access, Port Scanning, and Syn flood. Each Malicious Activity has features that can be a way to identify it. This paper attempts to investigate the malicious activities in the SCADA network running the IEC 60870-5-104 protocol. Raw traffic data from the SCADA network were recorded in pcap format. Next, by using Snort and Suricata software the characteristics of malicious activities are identified, and then observed using Wireshark software. The observation will produce attacks characteristics/features. Knowing these features will help to classify or to identify the attacks. In turn, the recognized features of the SCADA traffic network can be used to develop a machine learning model as a classifier engine in an intrusion detection system (IDS).**

Keywords*— *Features Recognition, Malicious Activity, SCADA, IEC 60870-5-104

I. INTRODUCTION

In modern SCADA, the SCADA system is connected to one or more other industrial protocols [1] thus opening many gaps to the threat of cyber attacks in the SCADA system [1],[2]. Cyber attacks on SCADA networks show an increasing trend with diverse and sophisticated techniques [3]. Because SCADA has an important role in communication on industrial devices so that all industrial system communication networks from field equipment to connecting network controllers and field devices such as PLC (Programmable Logic Controller) must be protected [4]. The vulnerability of the SCADA network/system pointed out by [5], finding more than 500,000 SCADA devices from various vendors can be accessed through the Shodan search engine if a SCADA device is connected to the heterogeneous network or the Internet.

Research work in [6] compares the IEC 60870-104 (IEC 104) protocol with other four protocols: Modbus, TASE.2, DNP3 and IEC-60870-5-101 protocols and states that of the four Authentication, Authorization, Integrity and Confidentiality features, the IEC 104 protocol only has Integrity features using Checksum, but more neither of the four protocols have these four complete features.

As the protocol that used in this work is IEC-60870-5-104, which in practice will be encapsulated into TCP protocol before being sent, the treatment in recognizing attack patterns in this protocol is not much different from recognizing traditional network attack patterns on TCP/IP protocol [7],[8]. The dataset used in experimenting with the malicious activity features is the dataset that resulted from a testbed network introduced by Maynard et al [9] which is still in the form of a .pcap file. This file will be read by using Wireshark software. This dataset contains traffic data of SCADA that running IEC-60870-5-104 communication protocol, and with performing a deeper analysis malicious activities such as Port Scanning, Syn Flood, and Unauthorized Access will be found.

In this study, the authors will show the characteristics of the malicious activity patterns in the SCADA network/system by displaying the payloads of these features using Wireshark from the results of the detection of Snort and Suricata software. Though the IEC 104 protocol has weaknesses, however, this protocol is widely used in industry [1],[10], especially the power plant industry. One of the reasons for the popularity of the IEC 104 protocol in the electrical industry is because the IEC 104 protocol supports Automation Generation Control (AGC) which is an algorithm that can regulate the balance of electrical energy in a large geographic area [1]. Thus, it is important to recognize early patterns of malicious activity which are useful for minimizing the threat of attack on the SCADA network/system.

The rest of the paper is structured as follows. In Section 2, the authors present research works related to pattern recognition in SCADA network/system. Section 3 describes the characteristics that can be used to recognize malicious activity in the dataset. In Section 4 the authors discuss the characteristics of the malicious activity and the function of these features as the results from observation. Lastly, Section 5 gives conclusions of this study and the authors plan on malicious activity in the future.

II. Related Work

Research conducted by [11] discusses data traffic patterns in the IEC 60870-5-104 protocol in the network by collecting data during the SCADA system operates and then using it to see the characteristics of Non-Polling Data. Data traffic analysis was carried out only on normal data without any attacks data in it. Figure 1 presents the IEC 104 protocol data frame format.

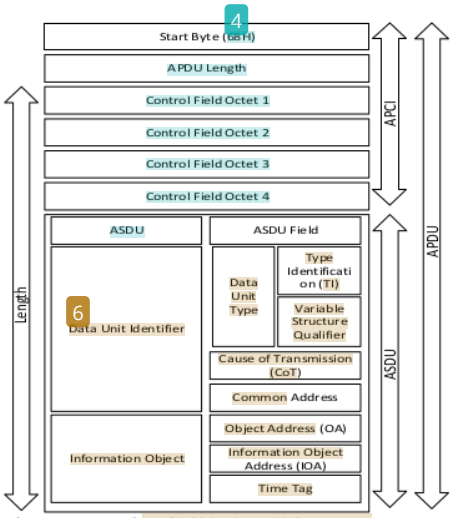

Fig 1. Protocol IEC 60870-5-104 Format

Research conducted by [12] uses a testbed system to simulate SCADA traffic then inserting malicious activities into it to be detected using the Snort and Suricata attack detection applications. This research was conducted to see the performance of the two attack detection applications then compare their performances.

In research work by [13], the authors simulate attacks on SCADA IEC 104 network, then measure the consequences of attacks on the SCADA system using Colored Petri Net (CPN). A study that discusses the correlation between the arrival time pattern of data packets and the SCADA Spontaneous Data Traffic to detect anomalies on the SCADA network has been carried out by [14]. This study is based on the results of a previous study by [11], Researchers find out that anomalies that occur in the data traffic of the SCADA system correlate with the Information Object Address (IoA) and Cause of Transmission (CoT) time patterns in the IEC 104 protocol, so that anomaly detection systems for SCADA network/ system can be built based on this correlation model.

III. Malicious Activity Pattern

The dataset used in this study is adapted from [9] and created from traffic data capturing of a testbed network that consists of nine hosts, namely: one Historian server device with an IP address of 10.50.50.151, one HMI device with an IP address of 10.50.50.150, five RTU devices with an IP address between 10.50.50.101 for RTU 1 to 10.50.50.105 for RTU 5, one reconnaissance device with IP address 10.50.50.3 and one Man in the middle Middle (MITM) device with IP address 10.50.50.99. In this study, the authors define a port scanning device as an illegal device on the network.

In the scenario, a MITM node is set up to send an invalid value for Causetx so that this becomes a feature to detect the invalid value using Snort and Suricata. Then several Suricata rules are modified to detect SYN Flood, Port Scan, Unauthorized Access and Invalid Cause of Transmission (CoT).

This study uses Snort software version 3.01 and Suricata software version 5.0.3 running on a Virtual Machine using Ubuntu 20.04 operating system and with a Virtual Machine specification of six CPU cores, 16 GB RAM and 64 GB Storage by detecting files. The two software work on the dataset with the pcap extension.

The results of the detection of Malicious Activity on the dataset using Snort and Suricata are Port scan activity, Syn Flood, Unauthorized Access and Invalid CoT and are presented in Table 1.

TABLE 1 SNORT AND SURICATA DETECTION RESULT

IDS Application	*Alert*	*Syn Flood*	*Port Scan*	*Unauthorized Access*	*Invalid CoT*
Snort	16183	4270	10.598	20	0
Suricata	17408	3596	10.598	50	1195

A. Syn Flood

Packets of SCADA communication network running IEC 104 protocol will be encapsulated into packets of TCP protocol before being sent [7][8]. There will be a three-way handshaking mechanism. thus, this mechanism is an opening door for an attacker to perform a Syn Flood Attack which allows the attacker to make multiple half-open connections to the target without sending an ACK [15]. Syn flood activity will be dangerous for devices that have low compute resources such as RTU devices on SCADA.

Snort and Suricata can detect Syn Flood warning packets in a total of 4270 warnings and 3596 warnings, respectively (see Table 1). In determining Syn Flood warnings the authors add a command for every 150 SYN data that arrives within 5 seconds it will be detected as Syn Flood attacks and will trigger alerts on Snorts and Suricata. Figure 2 shows the payload of one of the Syn Flood alerts detected in Suricata and Snort.

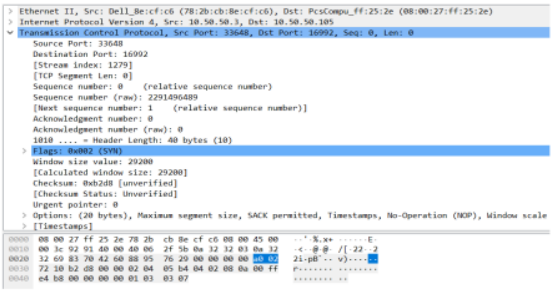

Fig 2. Syn flood Payload

All warnings that appear on Snort and Suricata are TCP Syn data packets sent to each RTU by the port scanning device.

B. *Port Scan*

Research works in [16] and [17] that discuss network defence system against port scanning has revealed that port scanning is the prefix of a cyber attack so it is important to detect it as early as possible. Similar to the two works, this study reveals the thing that triggers a port scanning warning on Snort and Suricata is the SYN packet from the original device then followed by the ACK and RST packets from the destination device. Figure 3 and Figure 4 displays the payload on the wireshark of the scanner and receiver devices, respectively.

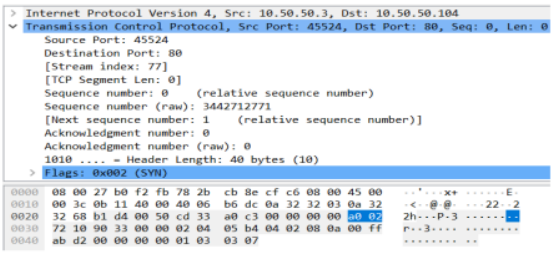

Fig 3. Syn Packet from port scanner device

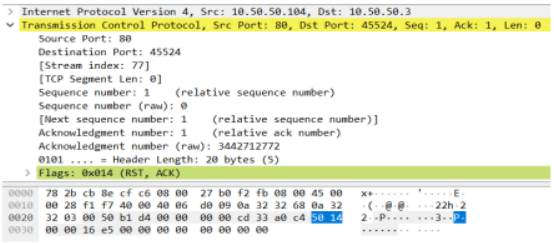

Fig 4. Reply RST and ACK from RTU

In the dataset, the port scanning device sends a SYN packet to each RTU to see the open ports, and the RTU replies with ACK and RST.

C. *Unauthorized Access*

The nature of the industry that uses SCADA protocols are reluctant to upgrade the system, and this matter will increase the vulnerability of cyber-attacks [13],[18]. Consequently, in addition to the weaknesses of the TCP/IP protocol, the weaknesses of the IEC 104 protocol also increase the vulnerability of the SCADA network. The weaknesses of the IEC 104 protocol include that the packets of the Application Data Layer are transmitted without an integrated encryption mechanism so that it allows attackers to perform analysis on the traffic data [6] and even to replace it. In this study, the authors apply the Application Protocol Control Information (APCI) with Utype TESTFR and STARTDT on Snort and Suricata to detect the features of Unauthorized Access, with the results of Snort successfully detecting 20 warnings and Suricata 50 warnings. These two packets are used as features, assuming the attacker will perform a control frame test to ensure the frame can be received by the RTU and then start the data transfer control. The TESTFR sent by the port scanning device and received by the RTU are shown in Figure 5 and Figure 6, respectively.

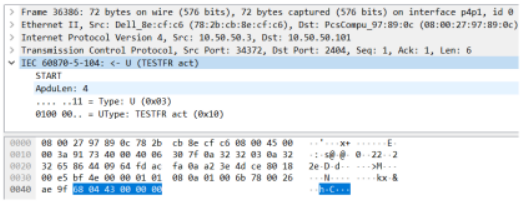

Fig 5. TESTFR act payload from Scanner Device

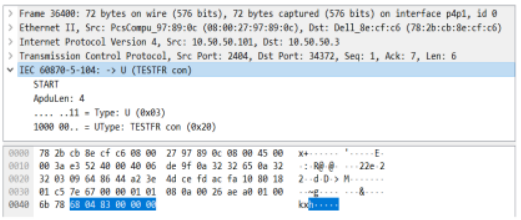

Fig 6. TESTFR con payload reply from RTU

The TESTFR act payload has *Utype ID 0x03* with a value of *0x10* and the reply from RTU TESTFR con has *Utype ID 0x03* with a value of *0x20*. The STARTDT payload sent by the port scanning device and received by the RTU is shown in Figure 7 and Figure 8, respectively.

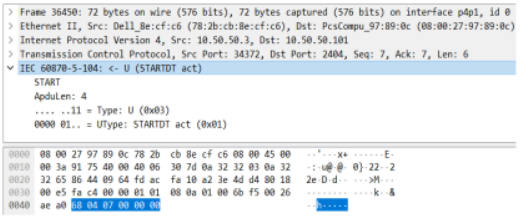

Fig 7. STARTDT act Payload form Scanning Device

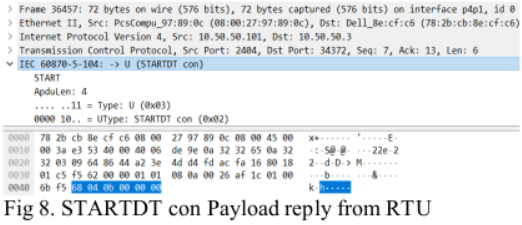

Fig 8. STARTDT con Payload reply from RTU

At payload STARTDT act has particularly *Utype ID 0x01* and *0x03* to the value of RTU TESTFR con reply has *Utype ID 0x03* to *0x02 value*.

D. *Invalid Cause of Transmission*

Cause of Transmission (CoT) is one of the attributes in the Application Service Data Unit (ASDU) that contains events or commands to the RTU. In the scenario in the dataset, the Cause of Transmission value is replaced with the Invalid Value [9] that occurred as a result of the MITM attack. In this study, the authors enter the value of Invalid CoT as a Malicious Activity because in general, the attacker would change the CoT value when he was able to enter the SCADA network system. Of the rules applied to Snort and Suricata, only Suricata displays warnings with a total of 1195 warnings. The payload of the warning is shown in Figure 9.

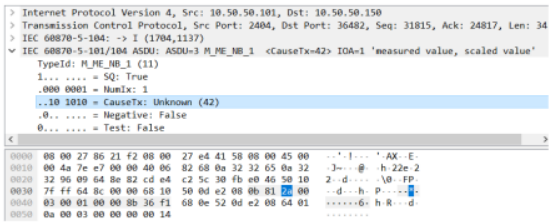

Fig 9. Invalid CoT payload from RTU

The CoT sent to the RTU with ASDU M_ME_NB_1 with a value of 42 is a value or code that is prepared for special instructions where its function is different in each industry, in testing the value of 42 has not been defined so that the recorded one has an unknown message (42). As for normal data in this dataset, ASDU M_ME_NB_1 will contain inrogen (20) as shown in Figure 10.

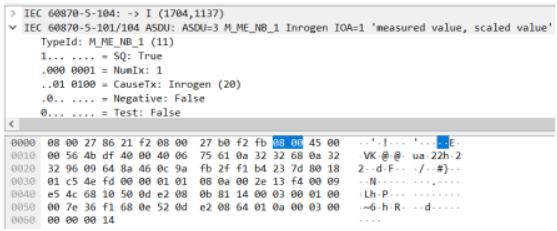

Fig 10. Valid CoT payload from RTU.

IV. Result and Discussion

From data observation, in detecting the Invalid value of CoT Snort cannot detect it even though the features entered for these conditions are the same as Suricata, of course with a little modification because the format of writing Snort and Suricata rules is slightly different. Figures 11 and Figure 12 show the rules for Suricata and the warnings that appear in Suricata.

```
alert tcp any 2404 -> any any (msg:"Protocol IEC 104 CoT Missing/Invalid Value"; flow:established; content:"|68|", depth 1; pcre:"/[\S\s]{5}(?![\x2D-\x33][\x3A-\x40][\x64-\x67][\x69|x6B|[\x6E-\x71])/iAR"; flags: A; content:!"|06|", offset 8, depth 1; classtype:bad-
```

Fig 11. Snort Rules for Detect Invalid CoT

```
04/10/2018-21:12:20.946480 [**] [1:6666611:1] Protocol IEC 104 CoT Missing/Invalid Value [**] [Classification: Potentially Bad Traffic] [Priority: 3] {TCP} 10.50.50.101:2404 -> 10.50.50.150:36482
```

Fig 12. Alert for Invalid CoT on Suricata

Likewise, when detecting Syn Flood attack and Unauthorized Access, Snort and Suricata get different results. Even though using the same rules the results of the detection of these two IDSs display different results, where Snort displays more warnings than Suricata, for detection of Unauthorized Access and Suricata displays more Unauthorized Access warnings than Snort. When performing Unauthorized Access detection, the author key in the APCI TESTFR and STARTDT conditions as conditions that trigger warnings on Snort and Suricata. Figure 13 displays the Rules for detecting Unauthorized Access conditions.

Snort Rule :

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT ACT"; flow:established; content:"|68|",depth 1; content:"|07|",within 1,distance 1; classtype:protocol-command-decode; sid:41047; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT CON"; flow:established; content:"|68|",depth 1; content:"|0B|",within 1,distance 1; classtype:protocol-command-decode; sid:41048; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR ACT"; flow:established; content:"|68|",depth 1; content:"|43|",within 1,distance 1; classtype:protocol-command-decode; sid:41051; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR CON"; flow:established; content:"|68|",depth 1; content:"|83|",within 1,distance 1; classtype:protocol-command-decode; sid:41052; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT ACT"; flow:established; content:"|68|"; depth: 1; content:"|07|"; within: 1; distance: 1; classtype:protocol-command-decode; sid:41047; rev:4;)

Suricata Rule :

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT CON"; flow:established; content:"|68|"; depth: 1; content:"|0B|"; within: 1; distance: 1; classtype:protocol-command-decode; sid:41048; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR ACT"; flow:established; content:"|68|"; depth: 1; content:"|43|"; within: 1; distance: 1; classtype:protocol-command-decode; sid:41051; rev:4;)

alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR CON"; flow:established; content:"|68|"; depth: 1; content:"|83|"; within: 1; distance: 1; classtype:protocol-command-decode; sid:41052; rev:4;)

Fig 13. Snort and Suricata rules to detect Unauthorized Access Condition.

Then from the observation of the results, besides the port scanning device, the registered devices such as HMI are also included in the warnings generated by Snort and Suricata, because HMI will indeed send APCI STARTDT to each RTU to perform Monitoring and Controlling functions, however, TESTFR only displays warnings from port scanning devices. This situation will be a problem if the preventive feature of these two IDS applications is activated because it will interfere with the communication between the HMI and the RTU. Figure 14 shows the results of the detection of TESTFR from Snort and Suricata and Figure 15 shows the results of STARTDT detection from Snort and Suricata.

Snort Alert :

04/10-19:50:40.963542 [**] [1:41051:4] "PROTOCOL-SCADA IEC 104 TESTFR ACT" [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {AppID: IEC 60870-5-104} {TCP} 10.50.50.3:52632 -> 10.50.50.102:2404

04/10-19:50:40.969624 [**] [1:41052:4] "PROTOCOL-SCADA IEC 104 TESTFR CON" [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {AppID: IEC 60870-5-104} {TCP} 10.50.50.102:2404 -> 10.50.50.3:52632

Suricata Alert :

04/10/2018-19:50:40.963542 [**] [1:41051:4] PROTOCOL-SCADA IEC 104 TESTFR ACT [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.50.50.3:52632 -> 10.50.50.102:2404

04/10/2018-19:50:40.969624 [**] [1:41052:4] PROTOCOL-SCADA IEC 104 TESTFR CON [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.50.50.102:2404 -> 10.50.50.3:52632

Fig 14. TESTFR alert from Snort and Suricata

Snort Alert :

04/10-19:50:41.4638963 [**] [1:41045:4] "PROTOCOL-SCADA IEC 104 STARTDT ACT" [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {AppID: IEC 60870-5-104} {TCP} 10.50.50.3:52632 -> 10.50.50.102:2404

04/10-19:50:41.465114 [**] [1:41046:4] "PROTOCOL-SCADA IEC 104 STARTDT CON" [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {AppID: IEC 60870-5-104} {TCP} 10.50.50.105:2404 -> 10.50.50.3:52632

Suricata Alert :

04/10/2018-19:50:41.463896 [**] [1:41045:4] PROTOCOL-SCADA IEC 104 STARTDT ACT [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.50.50.3:52632 -> 10.50.50.102:2404

04/10/2018-19:50:41.465114 [**] [1:41046:4] PROTOCOL-SCADA IEC 104 STARTDT CON [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.50.50.102:2404 -> 10.50.50.3:52632

Fig 15. STARTDT alert from Snort and Suricata

The rules for detecting Syn Flood Attack on Suricata and Snort are shown in Figure 16, there is no difference in the format of the rules for both and Figure 17 for the detection results on Snort and Suricata.

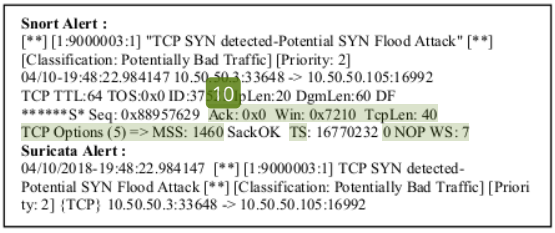

Fig 16. Snort and Suricata rules for detecting Syn Flood

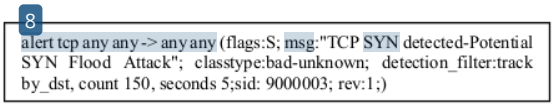

Fig 17. Alert for Syn Flood attack on Snort and Suricata

In detecting Port Scan, Snort and Suricata display the same detection results using the same rule without needing to be modified. In other words, the rule to detect Port Scan on Suricata can run on Snort. Figure 18 shows the rules used to detect Port Scan and Figure 19 shows the detection results of Snort and Suricata.

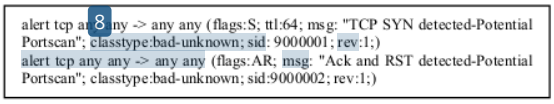

Fig 18. Snort and Suricata rule to detect Scanning Port

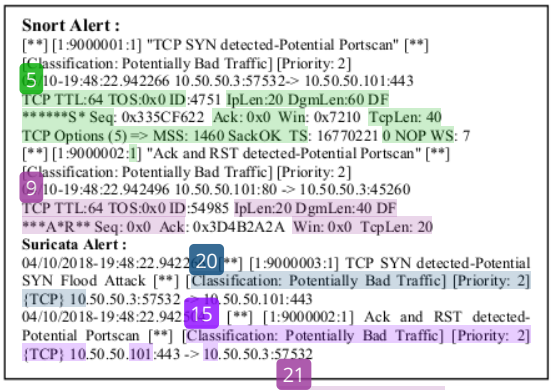

Fig 19. Alert for Port Scan on Snort and Suricata

The use of Snort and Suricata in detecting malicious activity has a weakness because it is still based on a signature base which depends on the set of rules in the database [19]. The use of Machine Learning techniques for more accurate results will be a good solution for detecting threats on the SCADA network. However, the use of a Signature-based IDS application can be used as a means to perform feature testing in detecting malicious activity but not for further application. Later, these features can be used in machine learning techniques.

From the obtained results, the authors will create a dataset that can be used for machine learning in detecting malicious activity based on the characteristics that exist in the dataset, to overcome the poor performance of Snort and Suricata in detecting malicious activity in this study. The characteristics that are suitable for each malicious activity scenario in this study will be used as the basis for developing a machine learning model in future studies.

The SYN attribute can be used as a feature/characteristic to detect a Syn Flood attack as mentioned by [20] that add an unknown IP address feature because data packets on the SCADA network are also encapsulated into TCP protocol packet format, before being sent.

Port scanning can also use the characteristics of the SYN packet but with the addition of a reply from the recipient with ACK and RST packets to improve the accuracy characteristics of an unknown IP address. In this study, Source Port feature as the target host and tcp flags to determine port scan activity originating from source ports in the SCADA network, namely a combination of SYN, ACK (0x12) flags, a combination of RST, ACK (0x14) flags and ACK (0x10) flags. The combination of SYN, ACK which is a response result from the target host, in this case, the RTU which indicates that the port is open [16]. Furthermore, as revealed by research work in [20] port scan can also be a feature for the detection of anomalies that occur due to port scanning activity. The authors characterize the target port where the port is generally widely used for various purposes in computer networks. Table 2 shows the ports used to determine the target port scan activity.

TABLE 2 SNORT AND SURICATA. DETECTION RESULT

Port	Information
2404	Default Port SCADA IEC 60870-5-104
5434	Default Postgre Port
5910	Default VNC Port
1521	Default Oracle Port
1433	Default MS SQL Port
3306	Default MY SQL Port
80	HTTP Port
8443 and 443	HTTPS Port
22	SSH Port

The TESTFR and STARTDT packets are official packages on the SCADA network using the IEC 60870-5-104 protocol but it will be dangerous if sent using an unknown device as in Figure 14 and 15 where STARTDT and TESTFR packets are sent by Reconnaissance devices. Unauthorized Access has APCI TESTFR and STARTDT features in its tracks. However, to avoid detection errors, an IP address-based feature will be added so that IP from official devices will not be detected as warnings in future machine learning models.

Invalid CoT in this study is not a feature of the attack, however, the ASDU value can be used as a feature to detect MITM because in ASDU there is a monitoring or control command that usually targets the target of cyber-attacks if CoT is added with information from the source IP address of the sender, and Information Object Address (IoA) from ASDU it can be used as a feature of a MITM attack..

V. Conclusion And Future Work

Attacks on SCADA networks, especially those that use the IEC-60870-5-104 protocol, still have the same types of attacks as traditional networks, such as port scanning and syn flood. Attacks on information contained in IEC 104 data frames still possible to be carried out with similar techniques as carrying out the attacks on traditional networks. Generally, with a little modification and knowledge of the IEC 104 protocol, the attacker can penetrate and launch various attacks on the SCADA network system, and it becomes special attention to authors in developing a reliable IDS.

In developing an IDS model with machine learning to detect attacks on a SCADA network, it is necessary to select the right features so that IDS can detect attacks accurately. From the data that has been obtained in this study, the authors recommend using the features of the data that have been tested using Snort and Suricata with the addition of several features such as unknown device and some IEC 104 data frame attributes to improve accuracy.

For future work, the authors think of conducting research on a system that is able to accurately detecting Unauthorized Access on SCADA networks running IEC 104 protocol by leveraging various machine learning algorithms and compare their performances to select the best one. Then extend the research to detect MITM attack detection on the SCADA network.

References

[1] K. Mai, X. Qin, N. Ortiz Silva, and A. A. Cardenas, "IEC 60870-5-104 network characterization of a large-scale operational power grid," *Proc. - 2019 IEEE Symp. Secur. Priv. Work. SPW 2019*, pp. 236–241, 2019, doi: 10.1109/SPW.2019.00051.

[2] P. Matoušek, O. Ryšavý, and M. Grégr, "Increasing Visibility of IEC 104 Communication in the Smart Grid," no. December 2015, pp. 21–30, 2019, doi: 10.14236/ewic/icscsr19.3.

[3] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, p. 101677, 2019, doi: https://doi.org/10.1016/j.cose.2019.101677.

[4] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Comput. Secur.*, vol. 87, p. 101561, 2019, doi: 10.1016/j.cose.2019.06.015.

[5] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly, and H. C. Chen, "Identifying Supervisory Control and Data Acquisition (SCADA) Devices and their Vulnerabilities on the Internet of Things (IoT): A Text Mining Approach," *IEEE Intell. Syst. 2018.*, pp. 1–11, 2018, doi: 10.1109/MIS.2018.111145022.

[6] A. Volkova, M. Niedermeier, R. Basmadjian, and H. De Meer, "Security challenges in control network protocols: A survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 619–639, 2019, doi: 10.1109/COMST.2018.2872114.

[7] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, and H. Soulsby, "A Forensic Taxonomy of SCADA Systems and Approach to Incident Response," pp. 42–51, 2015, doi: 10.14236/ewic/ics2015.5.

[8] W. Hou, X. Zhang, L. Guo, Y. Sun, S. Wang, and Y. Zhang, "Taxonomy of attacks on Industrial Control protocols," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9784, pp. 78–87, 2016, doi: 10.1007/978-3-319-42553-5_7.

[9] P. Maynard, K. McLaughlin, and S. Sezer, "An Open Framework for Deploying Experimental SCADA Testbed Networks," *Ics-Csr 2018*, no. 2016, pp. 89–98, 2017, doi: 10.14236/ewic/ics2018.11.

[10] E. M. Carlini *et al.*, "A new approach for sending dispatching orders using protocol IEC 60870-5-104," *2019 AEIT Int. Annu. Conf. AEIT 2019*, pp. 1–4, 2019, doi: 10.23919/AEIT.2019.8893376.

[11] C. Y. Lin and S. Nadjm-Tehrani, "Understanding IEC-60870-5-104 traffic patterns in SCADA networks," *CPSS 2018 - Proc. 4th ACM Work. Cyber-Physical Syst. Secur. Co-located with ASIA CCS 2018*, pp. 51–60, 2018, doi: 10.1145/3198458.3198460.

[12] H. Waagsnes and N. Ulltveit-Moe, "Intrusion detection system test framework for SCADA systems," *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-Janua, no. Icissp, pp. 275–285, 2018, doi: 10.5220/0006588202750285.

[13] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," no. June, pp. 41–46, 2019, doi: 10.1109/services.2019.00022.

[14] C. Lin and S. Nadjm-tehrani, "Timing Patterns and Correlations in Spontaneous SCADA Traffic for Anomaly Detection," *Raid 2019*, pp. 73–88.

[15] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 2, pp. 487–497, 2017, doi: 10.1109/TNSM.2017.2701549.

[16] M. S. Kumar, J. Ben-Othman, K. G. Srinivasagan, and G. U. Krishnan, "Artificial Intelligence Managed Network Defense System against Port Scanning Outbreaks," *Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019*, pp. 1–5, 2019, doi: 10.1109/ViTECoN.2019.8899380.

[17] N. Almasalmeh, F. Saidi, and Z. Trabelsi, "A dendritic cell algorithm based approach for malicious TCP port scanning detection," *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, pp. 877–882, 2019, doi: 10.1109/IWCMC.2019.8766461.

[18] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *J. Inf. Secur. Appl.*, vol. 34, pp. 197–204, 2017, doi: 10.1016/j.jisa.2016.05.007.

[19] D. Myers, S. Suriadi, K. Radke, and E. Foo, "Anomaly detection for industrial control systems using process mining," *Comput. Secur.*, vol. 78, pp. 103–125, 2018, doi: 10.1016/j.cose.2018.06.002.

[20] E. V. Ananin, A. V. Nikishova, and I. S. Kozhevnikova, "Port scanning detection based on anomalies," *11th Int. IEEE Sci. Tech. Conf. "Dynamics Syst. Mech. Mach. Dyn. 2017 - Proc.*, vol. 2017-Novem, pp. 1–5, 2017, doi: 10.1109/Dynamics.2017.8239427.

Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol

ORIGINALITY REPORT

11%
SIMILARITY INDEX

PRIMARY SOURCES

1	github.com Internet	86 words — 2%
2	Susanto, Deris Stiawan, M. Agus Syamsul Arifin, Mohd. Yazid Idris, Rahmat Budiarto. "IoT Botnet Malware Classification Using Weka Tool and Scikit-learn Machine Learning", 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), 2020 Crossref	57 words — 1%
3	softpanorama.org Internet	36 words — 1%
4	precyse.eu Internet	34 words — 1%
5	mt-fuji.ddo.jp Internet	29 words — 1%
6	www.scitepress.org Internet	29 words — 1%
7	eprints.unsri.ac.id Internet	23 words — 1%
8	Ric Messier. "Intrusion Detection Systems", Wiley, 2017	

	Crossref	20 words — < 1%
9	hdl.handle.net Internet	20 words — < 1%
10	T. Raja Sree, S. Mary Saira Bhanu. "Detection of HTTP Flooding Attacks in Cloud Using Dynamic Entropy Method", Arabian Journal for Science and Engineering, 2017 Crossref	16 words — < 1%
11	online-journals.org Internet	16 words — < 1%
12	Y-h. Taguchi, Turki Turki. "Tensor-decomposition-based unsupervised feature extraction applied to prostate cancer multiomics data", Cold Spring Harbor Laboratory, 2020 Crossref Posted Content	14 words — < 1%
13	www.cisco.com Internet	14 words — < 1%
14	export.arxiv.org Internet	13 words — < 1%
15	sublimerobots.com Internet	10 words — < 1%
16	www.fer.unizg.hr Internet	9 words — < 1%
17	"Telematics and Computing", Springer Science and Business Media LLC, 2020 Crossref	8 words — < 1%

18	Anna Volkova, Michael Niedermeier, Robert Basmadjian, Hermann de Meer. "Security Challenges in Control Network Protocols: A Survey", IEEE Communications Surveys & Tutorials, 2018 Crossref	8 words — < 1%
19	M. Agus Syamsul Arifin, Susanto Susanto, Deris Stiawan, Mohd Yazid Idris, Rahmat Budiarto. "The trends of supervisory control and data acquisition security challenges in heterogeneous networks", Indonesian Journal of Electrical Engineering and Computer Science, 2021 Crossref	8 words — < 1%
20	archive.org Internet	8 words — < 1%
21	dspace.cvut.cz Internet	8 words — < 1%
22	escholarship.org Internet	8 words — < 1%
23	theses.gla.ac.uk Internet	8 words — < 1%
24	G CLARKE. "Advanced considerations of IEC 60870-5", Practical Modern SCADA Protocols, 2003 Crossref	6 words — < 1%
25	Geeta Yadav, Kolin Paul. "Architecture and security of SCADA systems: A review", International Journal of Critical Infrastructure Protection, 2021 Crossref	6 words — < 1%
26	Tushar Ubale, Ankit Kumar Jain. "SRL: An TCP SYNFLOOD DDoS Mitigation Approach in Software-Defined Networks", 2018 Second International Conference on	6 words — < 1%

Electronics, Communication and Aerospace Technology (ICECA), 2018

Crossref

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF