The trends of supervisory control and data acquisition security challenges in heterogeneous networks

M. Agus Syamsul Arifin[1], Susanto[2], Deris Stiawan[3], Mohd Yazid Idris[4], Rahmat Budiarto[5]
[1, 2]Department of Engineering, Universitas Sriwijaya, Indonesia
[1, 2]Departenment of Computer Science, Universitas Bina Insan, Indonesia
[3]Department of Computer Science, Universitas Sriwijaya, Indonesia
[4]Department of Engineering, Universiti Teknologi Malaysia, Malaysia
[5]College of Computer Science & Information Technology, Albaha University, Al Baha, Saudi Arabia

Article Info

Article history:

Received Mar 19, 2020
Revised Dec 12, 2020
Accepted Jan 11, 2021

Keywords:

Distributed network protocol version 3
IDS SCADA
IEC 60870-5-104 (IEC 104)
SCADA protocol

ABSTRACT

Supervisory control and data acquisition (SCADA) has an important role in communication between devices in strategic industries such as power plant grid/network. Besides, the SCADA system is now open to any external heterogeneous networks to facilitate monitoring of industrial equipment, but this causes a new vulnerability in the SCADA network system. Any disruption on the SCADA system will give rise to a dangerous impact on industrial devices. Therefore, deep research and development of reliable intrusion detection system (IDS) for SCADA system/network is required. Via a thorough literature review, this paper firstly discusses current security issues of SCADA system and look closely benchmark dataset and SCADA security holes, followed by SCADA traffic anomaly recognition using artificial intelligence techniques and visual traffic monitoring system. Then, touches on the encryption technique suitable for the SCADA network. In the end, this paper gives the trend of SCADA IDS in the future and provides a proposed model to generate a reliable IDS, this model is proposed based on the investigation of previous researches. This paper focuses on SCADA systems that use IEC 60870-5-104 (IEC 104) protocol and distributed network protocol version 3 (DNP3) Protocol as many SCADA systems use these two protocols.

Corresponding Author:

Deris Stiawan
Department of Computer Science
Universitas Sriwijaya, Palembang, Indonesia
Email: deris@unsri.ac.id

1. INTRODUCTION

Cyber-attacks on industrial control system (ICS) including supervisory control and data acquisition (SCADA) tend to increase, with more diverse and sophisticated techniques [1]. These phenomena attract researchers to give more special attention to SCADA security issues [2]. The overall infrastructure in the industrial system, from field equipment to interconnection between control networks and field equipment controller such as programmable logic controller (PLC) is attempted to be protected [2]. SCADA security becomes a crucial issue due to the needs to quick and efficient access onto SCADA system currently available in the global market, so push the network service providers to provide and increase the capability of SCADA infrastructure to be accessed from the external heterogeneous network [3]-[5]. The need for more openness of the SCADA system opens up vulnerabilities in the SCADA system itself, as in research conducted by [1], [3], [4]. Researchers reveal security gaps in the SCADA system protocol itself that allow attackers to perform various attack scenarios on the SCADA system [6], [7].

Research work that aims to study the traffic data in the SCADA system have been carried out by [8]. The researchers investigate the normal traffic of the international electrotechnical commission (IEC) 104 protocol in the SCADA system. The research outcome contributes towards the development of defence model against the attack. Researchers in [9] find out an anomaly on the SCADA traffic when an attack on IEC protocol occurs.

Another research work in [10] uses a modelling technique called coloured petri nets (CPN) on DNP3 protocol and find the weakness in the security protocol used to broadcast message (DNP3-SA protocol). From the facts found in the experiments, the researchers in [10] conclude that SCADA needs an early alert system against any attacks on SCADA network, which is an intrusion detection system (IDS). However, there is a big challenge that obstructs research on IDS on SCADA system/network, which is the limitation of the available dataset [11].

This paper raises the issues related to IDSs in the SCADA network/system and gives a deep discussion on their security mechanisms through literature analysis. This analysis will increase the awareness of the security threats faced by the industrial world that implement SCADA system as the controller of equipment on their production processes. Besides, this paper will also discuss the issue of datasets that are currently an obstacle in SCADA security research, and then provides information on the crucial points on the SCADA network that can be used by attackers to explore malicious actions that may occur on SCADA systems. At the end of this paper, a conclusion from the discussion on the issues will be drawn, and things necessary to be done in the future to increase IDSs capability for SCADA system are recommended.

2. ANALYSIS OF ISSUES ON SCADA SECURITY

This section discusses issues related to SCADA security and factors that obstruct researches on SCADA security, such as the issue of vulnerability in the SCADA system and issues in the dataset. At the end of the section, based on the analysis and summary of the previous researches, the authors provide a general topology that reveals the crucial points that may be utilized to exploit the SCADA system.

2.1. Vulnerability issues of SCADA system

The more worrying cyber-attacks on SCADA networks, especially on strategic SCADA system such as an energy industry network will cause a dangerous impact on industrial devices. This worry was illustrated by a research carried out by Samtani *et al.* [12]. The researchers conduct research on search engine SHODAN and use text mining technique involving 578,000 out of 627,000,000 devices connected to a SCADA system through the internet of things (IoT) network. The finding was 37,845 devices are detected susceptible with various levels (critical, high, moderate, and low levels). The susceptible level is measured using Nessus software.

Researchers in [7] conduct experiments on attacking SCADA network, running IEC 104 protocol and the network is connected to the external heterogeneous network including IoT networks and find out holes for attacks. The researchers successfully perform IEC-104 flooding attack packet, TCP SYN DoS attack, unauthorized access, dan MiTM IEC 60870-5-104 isolation attack. This successful attack shows that opening the SCADA network connection that previously as closed network to other network running different protocols such as TCP/IP as stated by researchers [13]-[15] and IoT network protocols will open security holes of the SCADA system [16].

The weakness of the SCADA protocol itself can be a hole to be used by attackers to exploit the SCADA system as a result of research works on SCADA broadcast protocol DNP3-SA [10], [17]. The DNP3-SA protocol uses HMAC mechanism for the security; however, the mechanism is not so good enough in securing the broadcast message where the attacker is able to alter the broadcast message on DNP3-SAB protocol [17].

Researchers in [18] find out that by using supervised machine learning algorithm support vector machine (SVM), the encrypted data packet in SCADA network running DNP3 protocol can be classified. Thus, a man-in-the-middle (MiTM) on communication link can capture as well as remove the encrypted DNP3 packet data that already selected by the SVM, this is due to the opening of the SCADA connection to the Heterogeneous networks. Figure 1 illustrates the effect of SCADA network interconnection to external heterogeneous network as described by the above previous works [18].

2.2. Dataset issue

Researchers need solid benchmark dataset to support research on reliable IDS development. Wang *et al.* [19] find out many incorrect datasets because existing datasets were created with a lack of proper evaluation. Research work in [19] examines in depth the evaluation of the dataset that have five specific elements; input, controller, output, network, and attack. These elements are applied to a condition of the normal packet data and attack packet data on a testbed environment that represents the actual system. Ongoing Research on SCADA system is presented by Gómez *et al.* [20] about the methodology to generate anomaly detection datasets, the methodology is composed of four steps: attack selection, attack deployment, traffic capture and feature selection. The first and second steps indicate which and how to launch the attacks in the testbed, whereas the third and fourth steps deal with the capture of network traffic from the testbed and the extraction of relevant features.

Since the lack of available proper SCADA attacks dataset that publicly available, Maynard *et al.* [11] develop a SCADA network testbed that running IEC 104 protocol for creating a proper dataset. It consists of 9 hosts: 1 unit as human machine interface (HMI), 1 unit as data historian, 5 units as remote terminal units (RTUs), 1 unit as man in the middle (MiTM) attacker, and 1 unit as reconnaissance. The researchers use the attack scenario with MiTM attacker that targets the IEC 104 protocol by changing the cause of transmission (COT) value to an invalid value. The work focuses on the MiTM type of attack for changing the (COT) value, however many other attack types are carried out by other research works, such as in [9] which uses DoS Attack on IEC 104 protocol, and in [18] which uses injection and dropping attack on DNP3 protocol, researchers in [21] conduct experiments on reconnaissance, injection, masquerading, replay, and flooding attack on DNP3 protocol. In this case, the dataset used by [11] is not suitable for the use in other attack scenarios.

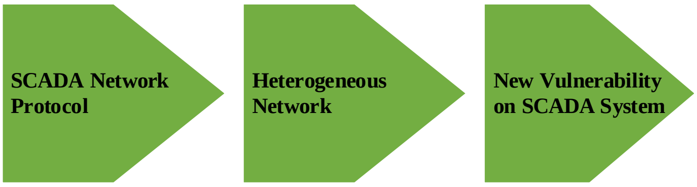

Figure 1. Effect of SCADA network interconnection with the heterogeneous network

2.3. Vulnerability SCADA on heterogeneous network

This section describes the general overview of security holes of the SCADA network that can be exploited to launch an attack on the SCADA system/network by using Figure 2 as an illustration. To make the observation easier the authors put five crucial points: A, B, C, D and E in Figure 2. The five points are the vulnerability holes where the attacker may use them to launch various attacks scenarios. Thus, to defend the network from the attacks, those points are selected to put IDS alarm sensors so the deployed IDSs become more efficient. Section 3 explains the details of the analysis for each point.

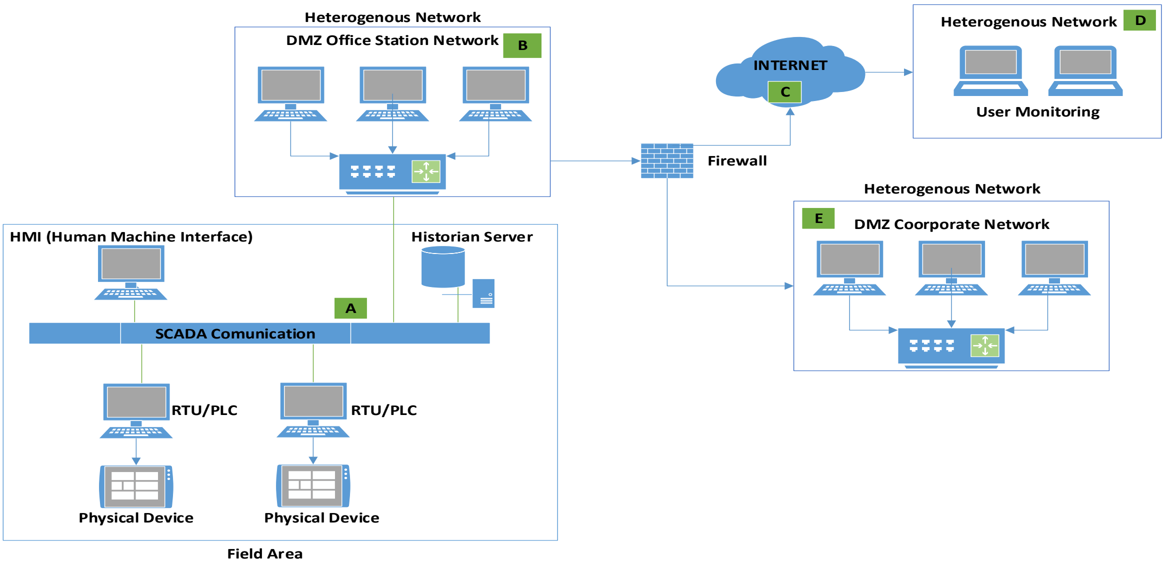

Figure 2. SCADA network topology example to describe security issues in the SCADA system

3. SECURITY ANALYSIS

In general data packet of SCADA protocol will be encrypted in TCP protocol before transmitted. [13], [15]. Therefore, the procedure to deploy an IDS on the SCADA network is not so different from the deployment on general TCP/IP networks. Nevertheless, before building and deploying an IDS on SCADA network, we have to know normal patterns of TCP data packets that contain SCADA protocol packets before understanding the data packet that contains an attack packet as proposed by Lin *et al.* [8] in understanding IEC 104 traffic patterns and Hodo *et al*. [9] for anomalies in the SCADA system on the IEC 104 protocol.

Subsection 3.1 discusses details of security holes in the five crucial points in Figure 2 that are used as a backdoor to exploit the SCADA system, subsection 3.2 discusses how the IDS alarm sensors are set up on those five points, so the IDS can work efficiently and accurately for detecting anomalies in the system SCADA networks and subsection 3.3 proposes a model for a future study to generate reliable IDS in the SCADA system.

3.1. Vulnerable points on general SCADA topology

The first vulnerability is at point A, where this point located in the area that having physical devices such as RTU device, HMI, and historian server as shown in Figure 3. MiTM attacker resides in the communication link can perform data dropping and change [18]. Besides, attack in the form of physical device attack most probably may happen in this point, since the attacker has already in the network that directly connects to the physical devices [7]. At this point, the attacker is able to monitoring and controlling industrial physical devices.

Point B is the closest location to the field area, monitoring and controlling are done by utilizing the SCADA protocol which is encrypted into the TCP protocol on a closed network, point E is a heterogeneous network located at the head office or branch that can perform monitoring and controlling PLC devices through the internet with VPN and tunneling lines. Point B and E on Figure 4, an attack that may happen is the attacker will try to find SCADA system vulnerabilities to penetrate the SCADA network/system and perform malicious activities.

As described in [7], possible attacks at point B and E that may happen are unauthorised access, DoS attacks and traffic analysis attacks. Attack to physical devices can be done from this point if the network device in this point is given access to control to the connected physical devices. Point C and D on Figure 5 the possible cyber-attack that may happen as discussed in [12] where the attacker looks for security holes on the SCADA system through an internet connection, especially on point D, where usually devices on this point only can monitor the status of physical devices.

In the case of an attack against user monitoring activities on this point, the attacker will perform Unauthorised Access attempt or be incognito as a device registered in the system to observe the activities of SCADA devices, in such a way, the attacker then expects to be able to identify the location of the physical device and observes any holes on the network that directly connect to the physical devices then trying to control industrial physical devices. DoS attacks at point C and D cause the performance of network devices not working optimally and can affect the communication connection between point E to point B which will be disrupted referring to the SCADA topology in Figure 2.

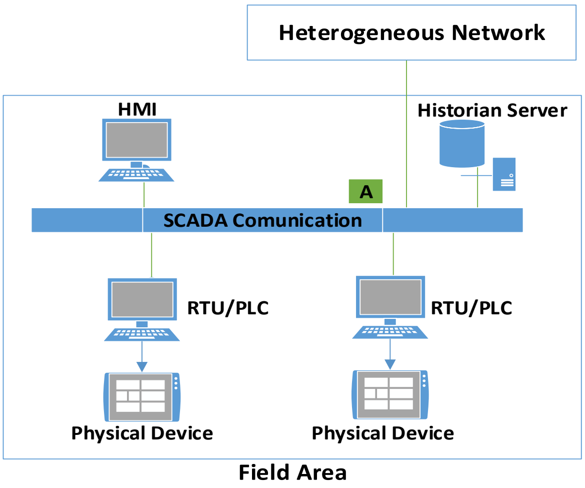

Figure 3. Vulnerable in the field area

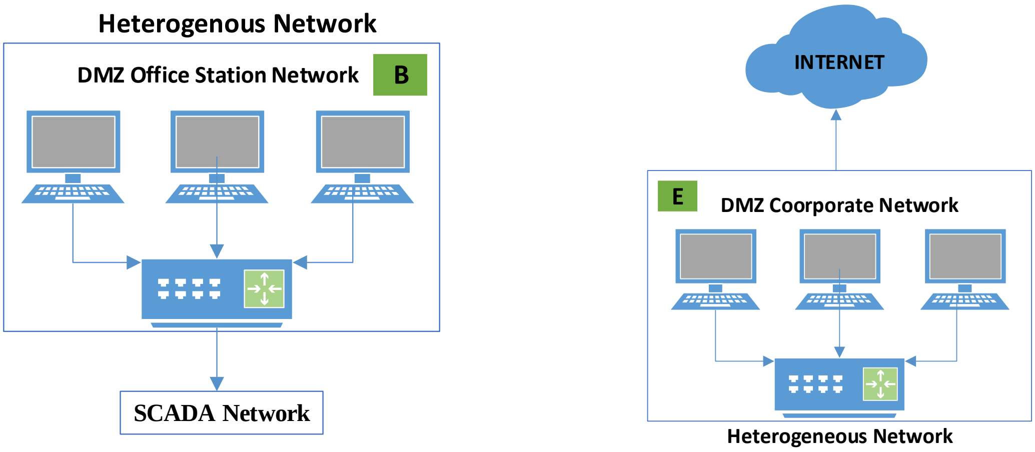

Figure 4. Vulnerability in the heterogeneous network in a SCADA topology

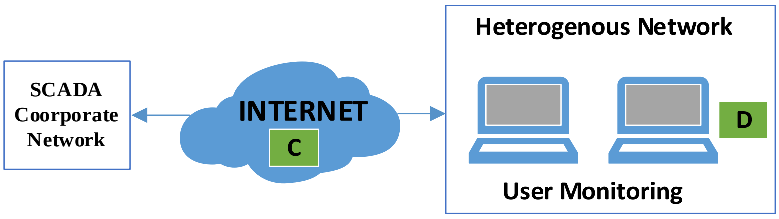

Figure 5. Possible cyber-attacks against SCADA system from the internet

3.2. Intrusion detection system alarm placement

Research works on IDS over SCADA system/network have been carried out including research works by [22]-[27] that use machine learning techniques, deep learning technique and IDS platform such as Suricata and Snort in the power plant and water treatment industry that uses the SCADA communication protocols on their SCADA systems. Various researches on IDS SCADA have been carried out, such as research by [22] that find out how to detect abnormal traffic in the generic object oriented substation event (GOOSE), manufacturing message specification (MMS) and sampled measure value (SMV) protocols used in the SCADA communication protocol. The use of machine learning algorithm to generating IDS on research by [23] explains how to use support vector machine (SVM) and deep belief network (DBN) to detect attacks on the combined SCADA-IoT platform. Research conducted by [24] explains how to classify attack data traffic and normal data traffic using SVM and RF algorithms to build IDS and then compare them along with the random hyper-parameter search results. Other studies [26] uses machine learning to produce IDS and performs comparisons of several machine learning algorithms, namely logistic regression (LR), random forest (RF), naive bayes (NB), decision tree (DT) and K-nearest neighbor (KNN). This work set up a testbed based on the SCADA system for water treatment and distribution with the results of the KNN as the algorithm that has the lowest performance in detecting attacks carried out in their experiments. Research work carried out by [25] simulates IDS on the SCADA framework to detect attacks on SCADA systems using Suricata and Snort to find which platform is suitable for detecting attacks on the framework used. Research that uses deep learning as an algorithm to build IDs on a SCADA system was carried out by [27] using the convolution neural network (CNN) algorithm to produce high accuracy in characterize salient temporal patterns of SCADA traffic and identify time windows where network attacks are present.

Other research works elaborate on attack patterns on the SCADA network include [9], [28], [29]. Nevertheless, those research works do not discuss the placement of the IDSs on SCADA network. Accurate placement of IDS sensors will produce a good early warning system for any SCADA network, so will minimize the disruption in the network/system by anticipating the attack entry points of the SCADA system. Figure 6 shows the locations for the IDS sensors be referring to a discussion on Figure 2.

A study on normal traffic pattern of SCADA network as conducted by research works in [9], [28], [29] is required to distinguish attack traffic pattern from normal traffic pattern [8]. IDS 1 in Figure 6 will detect attacks on physical devices that probably can remove even alter data packet on the SCADA system resides on the communication link of the SCADA network. As explained by the research work in [18], IDS 2 will detect cyber-attack on points A, B, C and D then IDS 3 will detect cyber-attack on point E of Figure 2. IDS 2 and IDS 3 detect unauthorised access, DoS attacks and traffic analysis attacks.

The placement of the IDSs aims to minimize the false detection and to make the deployed IDSs on SCADA network become more effective in detecting any anomalies on the SCADA network. Figure 7 is an illustration of how the IDS sensor works on the network like a SCADA network, the IDS sensor will detect abnormal data frames in data traffic on the network.

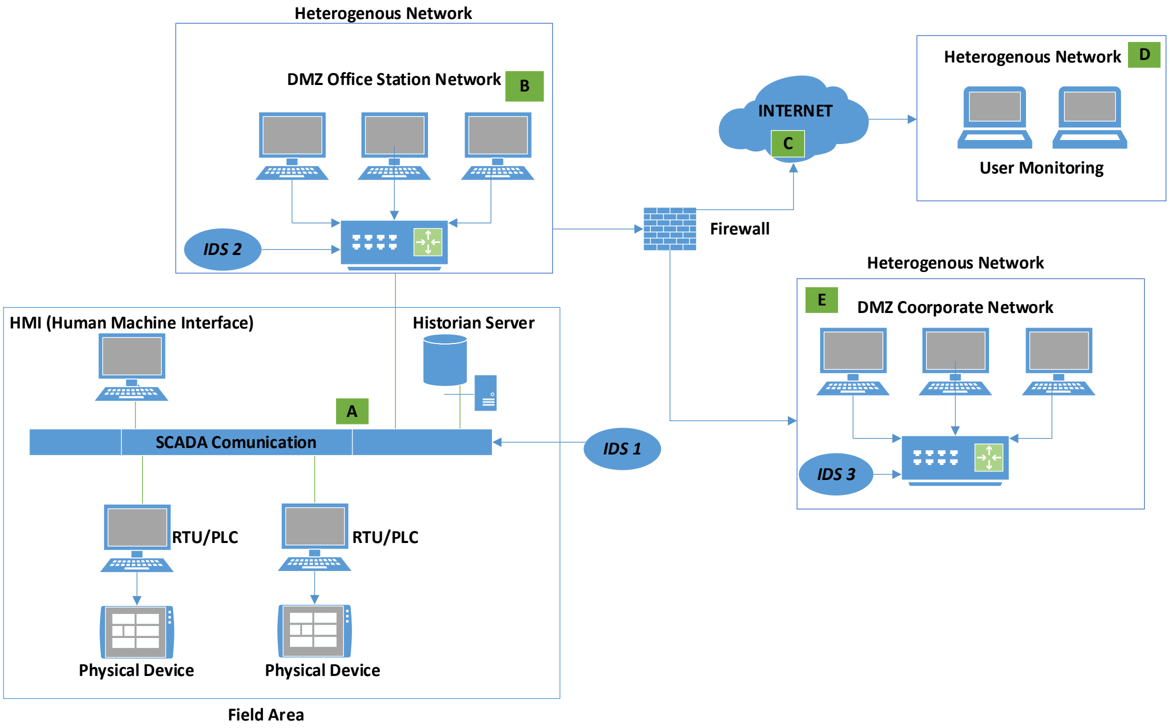

Figure 6. IDS sensor placement on SCADA network testbed example

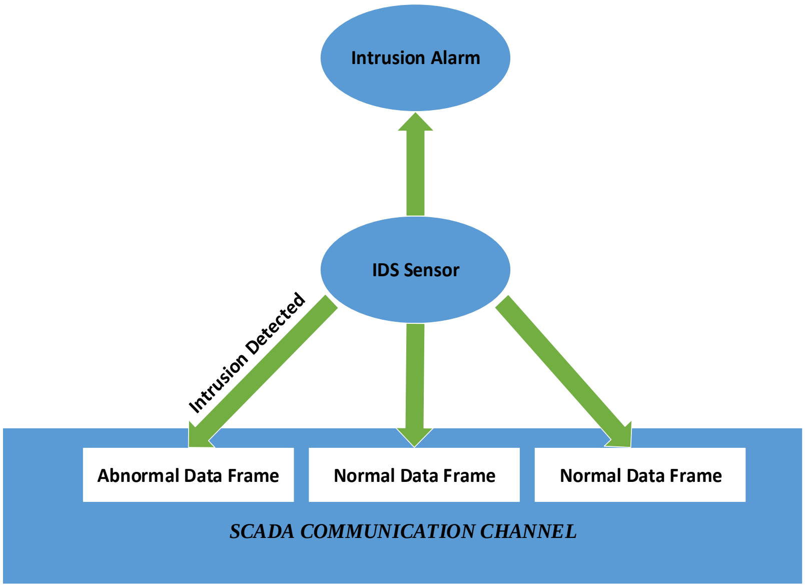

Figure 7. IDS sensor illustration in SCADA communication channel

3.3. The proposed model to generate reliable IDS

Figure 8 depicts a proposed model for our future study to build a reliable IDS. To get a good and proper dataset the main issues are on the setting of actual environment and actual attacks [19]. The main components of the dataset are the normal traffic and attack traffic. In the proposed model, the activity in creating dataset will pay attention to input, controller, network and attack scenarios used.

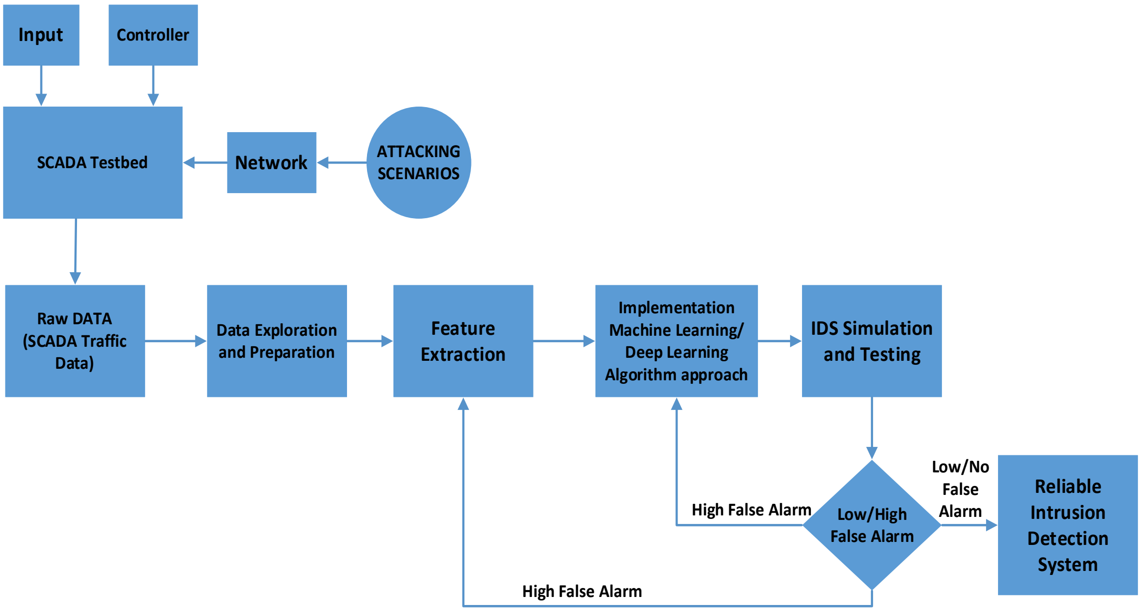
Input
Controller
SCADA Testbed
Network
ATTACKING SCENARIOS
Raw DATA (SCADA Traffic Data)
Data Exploration and Preparation
Feature Extraction
Implementation Machine Learning/ Deep Learning Algorithm approach
IDS Simulation and Testing
High False Alarm
Low/High False Alarm
Low/No False Alarm
Reliable Intrusion Detection System
High False Alarm

Figure 8. Proposed model for future study to generate reliable IDS for SCADA system

The Input section uses a device that carries out commands to provide certain conditions. In the SCADA system, the examples of input devices are sensor and human machine interface (HMI). In this model, the system will be created in a real environment on a laboratory scale so that it will produce real normal traffic data in the dataset. The controller device on the SCADA system is the main device component which is used to read inputs and generates outputs based on the program being executed. In the SCADA system, the controller device is PLC. The same as the input, the controller device will determine the quality of the dataset that will be generated. The network is a combination of input, controller and output which will simultaneously affect the real conditions in the model generated in the form of normal data packet traffic. In the case of the SCADA network, the system is the communication protocol used. After being able to produce normal data traffic patterns, an attack scenario is carried out to generate an attack data traffic pattern based on the scenario described in subsection 3.1 after security holes have been identified so that the attack scenario can be based on the vulnerability. The scenarios of attacks are executed to generate the attack data pattern on a dataset and will be based on the location of the vulnerability holes in the SCADA topology as presented in Figure 6, so that accurate attack data patterns will be obtained for the dataset.

The raw data generated from the scenarios carried out on the testbed will then be followed by the process of extracting features that had previously been done in data preparation. After the features of normal data traffic patterns and attack data, traffic patterns were obtained then feature selection algorithms that uses artificial intelligence techniques are deployed to build the IDS and conduct experiments with simulation to determine which artificial intelligence algorithm has a high level of accuracy and low false alarms.

The IDS models will be built were trained and generated to detect attack attempts on SCADA Network by using the training data. Consequently, the performances of the models were calculated. Table 1 depicts true positive (TP), true negative (TN), false positive (FP) and false negative (FN) statistics are used for the evaluation of model performances. Table 1 can be explained in the below items.

TN : Actual Normal is classified as normal.
FP : Actual Normal is classified as attack.
FN : Actual Attack is classified as normal.
TP : Actual Attack is classified as attack

Table 2 depicts accuracy, recall, precision and F1 score performance metrics are calculated using the statistics of the confusion matrix. The ratio of correctly predicted observations is accuracy, while precision means a ratio of correct positive observations. The recall is a proportion of correctly predicted positive events. F1 score signifies the weighted average of precision and recall.

Table 1. Confusion matrix

Actual Class\Predicted Class	Normal	Attack
Normal Data	TN	FP
Intrusion Activity	FN	TP

Table 2. Performance metrics

Measure	Formula
Accuracy	(TP+TN)/(TP+FP+FN+TN)
Recall	TP/(TP+FN)
Precision	TP/(TP+FP)
F1 score	2TP/(2TP+FP+FN)

4. CONCLUSION AND FUTURE WORK

As discussed, and agreed by many researches works on the threats against SCADA system security, it is concluded that the more we open the SCADA system towards external heterogeneous networks the more vulnerabilities are created that harm SCADA systems used by strategic industries. Therefore, countermeasures and steps to secure the system are required including the use of IDSs to detect an anomaly that happens in the SCADA system. However, to deploy reliable IDS a comprehensive and proper dataset is required. The correct IDSs placement may become an effective step in detecting attacks. Next, a study on recognizing SCADA network traffic pattern using artificial intelligence techniques is so important in which later on the recognition engine to be incorporated into visual attack detecting/monitoring software for future SCADA network/system. Improving the encryption methods ability that works well on SCADA system communication also becomes an aspect that can strengthen the SCADA system security. Both, the intelligent visual traffic monitoring as well as improved encryption techniques will become research focus of the future SCADA system security. In the near future, we plan to generate a new dataset with focus on DNP3 and IEC 104 protocols, which is widely used in industry, using testbed by paying attention to input, controller, and attack scenario. This testbed will simulate the SCADA System in the power plant industry based on the system of the power plant industry in Indonesia. The generated dataset will be used to build IDS using a machine learning algorithm or a deep learning algorithm approach.

REFERENCES

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

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

[3] M. R. Asghar, Q. Hu, and S. Zeadally, “Cybersecurity in industrial control systems: Issues, technologies, and challenges,” *Comput. Networks*, vol. 165, 2019, doi: 10.1016/j.comnet.2019.106946.

[4] 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.

[5] D. Upadhyay and S. Sampalli, “SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations,” *Comput. Secur.*, vol. 89, pp. 1-18, 2020, doi: https://doi.org/10.1016/j.cose.2019.101666.

[6] I. Darwish, O. Igbe, and T. Saadawi, “Vulnerability assessment and experimentation of smart grid DNP3,” *J. Cyber Secur. Mobil.*, vol. 5, no. 1, pp. 23-54, 2016, doi: 10.13052/jcsm2245-1439.513.

[7] 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.

[8] 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*, 2018, pp. 51-60, doi: 10.1145/3198458.3198460.

[9] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, “Anomaly detection for simulated IEC-60870-5-104 traffic,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, 2017, doi: 10.1145/3098954.3103166.

[10] R. Amoah, S. Camtepe, and E. Foo, “Formal modelling and analysis of DNP3 secure authentication,” *J. Netw. Comput. Appl.*, vol. 59, pp. 345-360, 2016, doi: 10.1016/j.jnca.2015.05.015.

[11] 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.

[12] 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.

[13] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, and H. Soulsby, “A Forensic Taxonomy of SCADA Systems and Approach to Incident Response,” *3rd International Symposium for ICS & SCADA Cyber Security Research 2015*, 2015, pp. 42-51, doi: 10.14236/ewic/ics2015.5.

[14] S. Nazir, S. Patel, and D. Patel, “Assessing and Augmenting SCADA Cyber Security- A Survey of Techniques,” *Comput. Secur.*, 2017, doi: 10.1016/j.cose.2017.06.010.

[15] 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.

[16] A. Sajid, H. Abbas, and K. Saleem, “Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges,” *IEEE Access*, vol. 4, pp. 1375-1384, 2016, doi: 10.1109/ACCESS.2016.2549047.

[17] R. Amoah, S. Camtepe, and E. Foo, “Securing DNP3 Broadcast Communications in SCADA Systems,” *IEEE Trans. Ind. Informatics*, vol. 12, no. 4, pp. 1474-1485, 2016, doi: 10.1109/TII.2016.2587883.

[18] T. de Toledo and N. Torrisi, “Encrypted DNP3 Traffic Classification Using Supervised Machine Learning Algorithms,” *Mach. Learn. Knowl. Extr.*, vol. 1, no. 1, pp. 384-399, 2019, doi: 10.3390/make1010022.

[19] X. Wang and E. Foo, “Assessing Industrial Control System Attack Datasets for Intrusion Detection,” *2018 3rd Int. Conf. Secur. Smart Cities, Ind. Control Syst. Commun. SSIC 2018 - Proc.*, 2018, pp. 1-8, doi: 10.1109/SSIC.2018.8556706.

[20] Á. L. P. Gómez *et al.*, “On the Generation of Anomaly Detection Datasets in Industrial Control Systems,” *IEEE Access*, vol. 7, pp. 177460-177473, 2019, doi: 10.1109/ACCESS.2019.2958284.

[21] N. R. Rodofile, K. Radke, and E. Foo, “Framework for SCADA cyber-attack dataset creation,” *ACM Int. Conf. Proceeding Ser.*, 2017, doi: 10.1145/3014812.3014883.

[22] Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks,” *IEEE Trans. Power Deliv.*, vol. 32, no. 2, pp. 1068-1078, 2017, doi: 10.1109/TPWRD.2016.2603339.

[23] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, “Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,” *Appl. Soft Comput. J.*, vol. 71, pp. 66-77, 2018, doi: 10.1016/j.asoc.2018.06.017.

[24] R. Lopez Perez, F. Adamsky, R. Soua, and T. Engel, “Machine Learning for Reliable Network Attack Detection in SCADA Systems,” *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, 2018, pp. 633-638, doi: 10.1109/TrustCom/BigDataSE.2018.00094.

[25] 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, 2018, pp. 275-285, doi: 10.5220/0006588202750285.

[26] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, “SCADA system testbed for cybersecurity research using machine learning approach,” *Futur. Internet*, vol. 10, no. 8, 2018, doi: 10.3390/fi10080076.

[27] H. Yang, L. Cheng, and M. C. Chuah, “Deep-Learning-Based Network Intrusion Detection for SCADA Systems,” *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, 2019, pp. 1-7, doi: 10.1109/CNS.2019.8802785.

[28] M. Kalech, “Cyber-attack detection in SCADA systems using temporal pattern recognition techniques,” *Comput. Secur.*, vol. 84, pp. 225-238, 2019, doi: 10.1016/j.cose.2019.03.007.

[29] F. A. Alhaidari and E. M. Al-Dahasi, “New approach to determine DDoS attack patterns on SCADA system using machine learning,” *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, 2019, pp. 1-6, doi: 10.1109/ICCISci.2019.8716432.

BIOGRAPHIES OF AUTHORS

M. Agus Syamsul Arifin received his master degree in Computer Science from Universitas Bina Darma Palembang, South Sumatera, Indonesia. Currently, he is a PhD candidate at Faculty of Engineering, Universitas Sriwijaya. He is currently a senior lecturer at Faculty of Computer, Universitas Bina Insan, Indonesia. His research interests include a computer network, information technology, information security, and network security.

Susanto received his master degree in Computer Science from Universitas Bina Darma Palembang, South Sumatera, Indonesia. Currently, he is a PhD candidate at Faculty of Engineering, Universitas Sriwijaya. He is currently a senior lecturer at Faculty of Computer, Universitas Bina Insan, Indonesia. His research interests include cryptography, information technology, information security, and network security.

Deris Stiawan received the PhD degree in Computer Engineering from Universiti Teknologi Malaysia, Malaysia. He is currently an Associate Professor at the Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya. His research interests include a computer network, Intrusion Detection/Prevention System, and heterogeneous network

Mohd Yazid Idris is an Associate Professor at School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia. He obtained his M.Sc and PhD in the area of Software Engineering, and Information Technology (IT) Security in 1998 and 2008 respectively. In software engineering, he focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of Intrusion Prevention and Detection (IPD).

Rahmat Budiarto received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng. and Dr.Eng. in Computer Science from Nagoya Institute of Technology in 1995 and 1998, respectively. Currently, he is a Full Professor at the College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include intelligent systems, brain modelling, IPv6, network security, wireless sensor networks, and MANETs.