International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.466

A Mapping Study of Intrusion Detection System

Wan Ahmad Safwan Wan Umar, Norsaremah Salleh*
Computer Science Department, Kulliyyah of ICT, Malaysia

*Corresponding author norsaremah@iium.edu.my
(Received: 28th March 2024; Accepted: 4th April 2024; Published on-line: 30th July 2024)

Abstract—The Network Security Monitoring System has been widely used to check many systems that supply services. A lot of monitoring tools have been developed to facilitate the monitoring of the network security. Since there are a lot of options to cater to our needs, this will cause a lot of time and resources to try each tool that is suitable with the system. In this research, we conducted a comparative analysis to analyse each tool presenting their advantages, disadvantages and the method used. The main objective of this research is to perform a systematic mapping study for the purpose to identify research topics related to network intrusion detection system, to assess the most frequently applied method of intrusion detection system, and to verify the types of cyber-attack that currently exist. Based on the 30 primary studies included in this mapping study, the findings indicated that the most intrusion detection system commonly used is the hybrid method and Data Injection has been the primary attack type in the existing system.

Keywords—Intrusion detection, attack detection, mapping study, types of attack

I. Introduction

Attack detection systems or Intrusion detection systems (IDS) are a vital component of cybersecurity, as they help organizations identify and respond to threats in their networks and systems [1]. An IDS focuses on traffic that is on the internal network to identify any suspicious or malicious behavior, in contrast to a firewall, which is at the perimeter and serves as a gatekeeper to monitor network traffic and assess if it should be allowed into the network or endpoint at all. As a result, the IDS is able to identify attacks that bypass the firewall as well as those that come from within the network. Most IDS solutions combine anomaly-based detection, which simply searches for suspicious activity or behavior that is strange or significantly different from the established norm, with signature-based detection, which compares traffic against a database of known attacks or attack techniques, to detect threats [1].

Why do we need IDS when we already have firewall? Mihret et al. [1] mentioned, "*No network is impermeable, and no firewall is error-proof. Attackers often create new vulnerabilities and attack methods intended to get past your security*". For many attacks, obtaining user credentials that give them access to the network and data requires the deployment of other malware or social engineering. Network security requires a network intrusion detection system (NIDS) since it makes it possible to identify and react to hostile traffic. However, the landscape of attack detection systems is vast and varied, with numerous approaches, techniques, and technologies available. As a result, it can be difficult for organizations to determine which attack detection system is the most appropriate for their needs [2].

The main objectives of this study are: i) to investigate the publication fora on the network intrusion detection system; ii) to identify the most frequently applied method of intrusion detection system, and iii) to verify the existing types of cyber-attack. This mapping study aims to provide a comprehensive overview of the current state of the field of attack detection systems, including the various approaches, techniques, and technologies that are used, as well as their strengths and limitations. The goal of this research is to help organizations make informed decisions about which attack detection system is the most suitable for their needs, based on a thorough understanding of the available options. In this study, the research was conducted to explore existing research on attack and intrusion detection systems. In addition, the research was conducted by producing a research question to guide to search for the sources of academic literature that relate to the subject matter.

This paper is organized as follows: Section 2 describes the related work available in relation to intrusion detection system. Section 3 describes the research methodology whereas Section 4 presented the analysis of results. Section 5 presented discussion of the findings in terms of research trends and gaps. Finally, Section 6 concludes this study.

II. Related Work

This Section describes the existing research works related to intrusion detection system. Vuong et al. (2015) studied a decision tree-based approach to generate basic detection criteria that are tested against denial of service and command injection attacks [3]. They discovered that adding physical input features could significantly minimize false positives and improve overall detection accuracy. They also developed an intrusion detection system that considers not

https://doi.org/10.31436/ijpcc.v10i2.466

only cyber inputs like network traffic and disc data, but also physical inputs like speed, physical jittering, and power consumption.

Wu et al. (2021) presents a unified method, in the sense of sharing the DDAE models, to provide simultaneous eavesdropping defense and detection of three common CPS attacks [4]. The simulation resulted the IEEE bus-57 system that demonstrates the proposed encryption-decryption strategy. It helps to accomplish secure transmission while maintaining acceptable reconstruction errors.

An et al. (2022) investigated the attack strategy against the power grid's dynamic state estimation, which is first presented from the adversary's point of view. The authors also identified the problem of detecting data integrity attacks, which is formulated as a partially observable Markov decision process with the feature of sequential decision-making. In the same study, a deep reinforcement learning-based method is also suggested for detecting data integrity attacks, which makes use of the Long Short-Term Memory layer to extract the state features from earlier time steps to determine whether the system is currently under attack [2].

Based on the review of related literature, we did not find any similar study that has performed review of related primary studies on the topic of intrusion detection system. Hence, this mapping study serves as a secondary study that will focus on empirical or primary studies looking at solutions on the intrusion detection.

III. Research Methodology

Systematic Mapping Study (SMS) methodology was utilized to identify and synthesize the studies found in the area of intrusion detection system. SMS method will help us to carry out a thorough, in-depth systematic method in performing the study. We refer to the mapping study guidelines by Petersen et al. 2008 [5]. SMS is described as the process of identifying and classifying existing literature publications that are pertinent to the research objective. This research major objective is to gain a thorough understanding of a certain study issue by evaluating recent and related work, identifying and analyzing research gaps and trends of intrusion detection system. The process involved in conducting the mapping study is shown in Fig. 1.

In the planning phase we formulated the research questions in order to provide an overview of the research field. Then in the second phase we started with searching the relevant primary studies. There are a few steps to conduct the searching of studies, such as specifying search string, list down online databases, manual hand searching and lastly snowballing technique. After conducting the search of relevant resources, we performed screening of all studies that have been retrieved using the inclusion and exclusion criteria. Then the classification of all the collected studies, general classification, and topic dependent classification were identified. Finally, relevant data from selected primary studies were extracted for analysis.

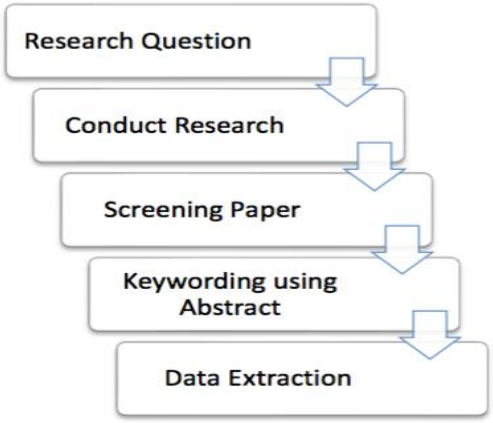

Fig. 1 Systematic Mapping Process

The first crucial stage in developing a structure for categorizing all relevant evidence obtained is the formulation of research questions (RQs). Since this study is designed to draw on empirical data to comprehend the research issue, a PICOC framework has been used to help us frame the research questions [6]. The PICOC that stands for Population, Intervention, Comparison, Outcomes, and Context, has been identified as can be seen in Table 1.

TABLE I
PICOC

Population	IT/SE companies
Intervention	Intrusion Detection System (IDS)
Comparison	Types of attack
Outcomes	Trends and gaps of the research studies
Context	Network security empirical studies

Based on the PICOC structure, we developed the following research questions (RQs) together with their accompanying justifications:

Research Question 1: What are the research topics that have been discussed in the studies of intrusion detection system?

Rationale: Since our focus is on the Attack detection system used in network security, it has required us to focus onto investigating what are available topics that have been written so far in the academic literature. The studies must clearly clarify on the attack detection system technologies used in their system. From this question, it gives an outline for us to analyze the IDS founds.

Research Question 2: What is the most frequently applied method of intrusion detection system?

https://doi.org/10.31436/ijpcc.v10i2.466

Rationale: The purpose of this question is to look into the publication patterns that can be inferred from publication information, such as the journal where the studies were published, the publication venue where we can determine who the research papers' intended audiences are, and the publication year where we can determine when academic researchers first began to study this particular subject and how it relates to current trends of network security.

Research Question 3: What are the types of attack that IDS are dealing with?

Rationale: This sub-RQ gives us an extra edge on what type of situation relates in the paper and how it gives better understanding in this certain area.

A. Study Procedures

The second stage of the SMS research methodology involved conducting a search of primary studies. The two main tasks required are defining search strings and applying them to the chosen online databases. Based on the specific terms and their comparable or synonym words identified from the study questions, we created the search string. We have used the following search string: network detection AND security AND (IDS OR system)

In order to identify additional publications from the original research discovered, we also used the backward snowballing technique through this process, which entails inspecting the references of all retrieved papers that are available. There are seven (7) papers retrieved through this technique based on the references list. In terms of the available online databases, we have used IEEEXplore and Scopus as our main resources to perform the search process in order to discover primary studies. The search string created earlier for the database search was used to carry out this action.

B. Screening of Papers

The next step is to screen the papers obtained from the searching of studies. The process of selecting papers that address the relevant parts of the subject is known as screening paper, and it is used to further filter out the papers that will be used in answering the RQs.

Additionally, SMS has defined goals and questions, and inclusion and exclusion are essential components that serve as criteria for choosing the right materials to be included or excluded. Both of the requirements should be considered based on the following categories, in accordance with "study population, nature of the intervention, outcome variables, time period, cultural and linguistic range, and methodological quality" **Error! Reference source not found.**.

We selected articles for inclusion based on the following selection criteria:

1. Studies must directly relate to intrusion detection system in a cyber security network.
2. Studies must provide adequate supporting details on how the attack was carried out and what system was affected.
3. Studies must be written in English.

In order to further filter the studies, the papers were removed based on the following exclusion criterion:

1. Studies focus on the attack instead of the detection system.
2. Studies that do not provide any empirical data.
3. Studies that are too short or brief such as abstract, poster etc. that did not provide any significant evidence.

C. Keywording of Abstracts

A step in categorizing the plan to produce the categories is known as keywording of abstracts. The purpose of this process is to provide information that supports studies resulting from the categorization activity. There are two approaches known as general classification and topic-specific classification.

The selected studies are categorized according to publication venues and publication years under general classification, often known as topic independence. In addition to the general classification, the topic-specific classification is also utilized, in which the articles are divided into groups according to the types of application. The classification, which is referenced in Table 2, can also be referred to as topic-dependent because it is associated with and dependent on a specific goal of categorization based on the topic matter.

TABLE II
Classification Scheme

General Classification	Topic-dependent Classification
Publication venue Publication year	Method of IDS Types of attack Study method

D. Data Extraction

As the last step, the classification system is used to map all of the primary studies to extract the data that is related to the research questions. To manage citations and determine publication frequencies to aid in identifying the most recent study topic, all data are organized into tabular form and stored in an Excel spreadsheet. We have extracted the following types of data: a) author(s) name, b) the year the work was published, c) paper title, d) research topic, and e) research method. Data extraction also covers IDS mechanism and the form of attack while mirroring the study questions.

https://doi.org/10.31436/ijpcc.v10i2.466

IV. Analysis of Results

We discovered 29 publications as a consequence of the search string procedure, of which 25 papers were retrieved from IEEE Explore and 5 from Scopus. The snowballing process further identified 7 papers. Finally, when applying the inclusion and exclusion criteria, we selected only 30 studies for data extraction process. Fig. 2 illustrated the selection process of the studies based on the inclusion and exclusion criteria identified in this study.

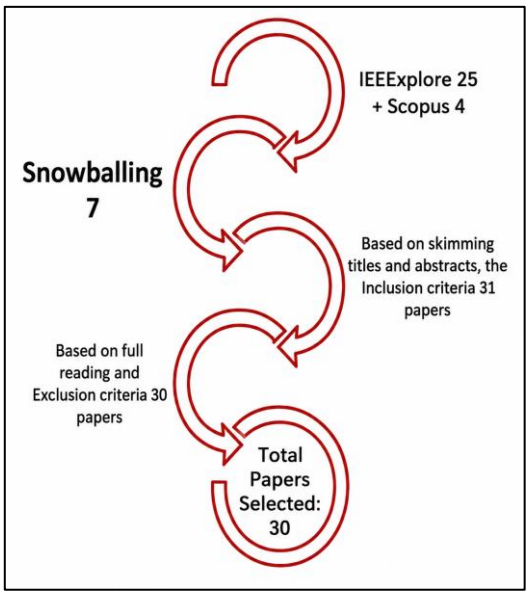

Fig. 2 Papers Screening

A. Answering Research Question 1 (RQ1)

This question allows us to have an overview of the current subject that has been covered between 2015 and 2022. This mapping study yielded a total of 20 topic subjects related to IDS, demonstrating the broad range of topics that an intrusion detection system ought to cover. Table 3 provides the topic discussed in the selected studies. We found that most of the studies (11 papers) fall under the topic of cyber physical systems.

TABLE III
Topic Discussed

Topic discussed	Study(s)
Cyber physical system	[7], [17], [20], [21], [23], [25], [26], [27], [30], [31], [35]
Smart Grid system	[8]
Power system	[9], [24]
Unmanned Aerial Vehicles UAVs	[10]
Delay Tolerance System	[10]
Factory Interface Network	[11]
Dynamic Watermarking	[12]
Close loop Robotic system	[13], [15], [19]
Actuator Deception	[14]
Neural Network	[18]
Networked Control System	[19]
Automatic Generation Control	[20]
Nonlinear System	[21]
Blockchain	[24]
Web Application	[28]
Smart Island	[29]
Data Driven Security	[32]
Multi Area Power System	[33]
Mobile Cyber physical system	[34]
Deep Learning	[36]

B. Answering Research Question 2 (RQ2)

From the mapping study we have acquired a total of 30 papers that mentioned all the methods they used in intrusion detection system. Table 4 shows the results of the analysis. Anomaly-based IDS capable to detect intrusion in both network and computer via monitoring of system's activity and then classify them as either normal or anomalous. The signature-based IDS examines the network traffic and compares it with known signatures, while hybrid method combines both the anomaly and signature-based approaches to enhance the effectiveness of intrusion detection. The hybrid method appeared to be the most used method in the IDS study, followed by anomaly-based IDS.

TABLE IV
Methods of IDS

Method of IDS	Study(s)
Anomaly Based IDS	[7], [13], [16], [18], [19], [20], [22], [30]
Signature Based IDS	[8], [14], [21], [23]
Hybrid	[9], [10], [11], [12], [17], [25], [28], [31], [34], [35], [36]

Figure 3 shows the number of IDS methods used throughout the papers acquired. Based on the figure we can see that hybrid method has the highest number that is 11 studies compared to the other method. Although the number of signatures based has the lowest which is 4 papers, the studies that report this type of method presented detail study explaining how this method helps them get through their problems.

https://doi.org/10.31436/ijpcc.v10i2.466

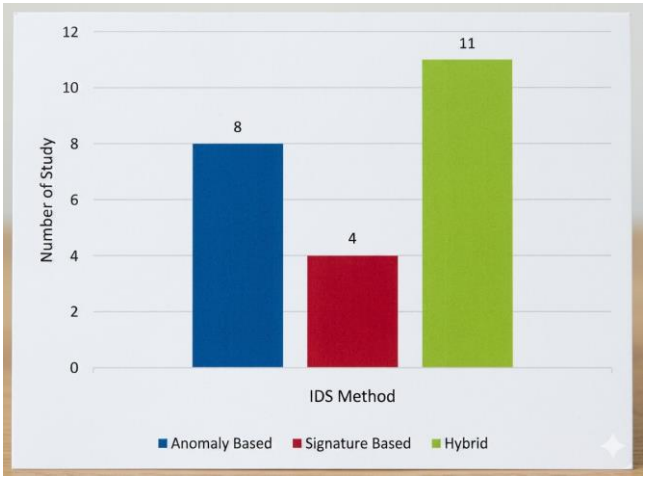

Fig. 3 Types of IDS method used

There are not many usages on the signature based because of a certain reason. Based on our analysis, we found that signature based method has weakness that is it only focused on specific attacks and it can only deal with known attacks [8]. A signature is essentially the attack's unique fingerprint. The action is captured by the signature, which is exclusive to a given attack. This practical technique is targeted at certain attacks and particularly effective at reducing the number of false positives.

On the other hand, a behavioral approach or anomaly-based method places less emphasis on a specific attack pattern and more on user or application behavior. Differentiating between harmful and non-malicious behaviors is the aim. Such systems have enormous promise: This kind of defense can theoretically counteract any attacks, both known and undiscovered. Since there are no attack signatures used, it also claims to relieve the user of the need to keep the system updated.

The finest features of both protection approaches are combined in a hybrid approach, which is the most effective defense against attacks. By offering protection against both known and unknown assaults and suppressing false-positive rates, these hybrids overcome the basic trade-off. Managers must ultimately choose what is the most crucial method to safeguarding the servers, data, and files in their settings. A hybrid strategy calls for protection at all tiers to guarantee that sensitive data is not jeopardized.

C. *Answering Research Question 3 (RQ3)*

Table 5 shows the list of attacks and Figure 4 shows the frequency of the attack from the data we extracted from the selected studies. We can see that there are a total of 11 types of attack (see Table 5). The most frequent attack is the data injection with the total number of 8, followed by the general attack with a number slightly lower than data injection, which are 7 studies. All other types of attack are significantly smaller number with 1 study mention each except for the denial of service with 4 studies mentioned by the research paper.

TABLE V
Types of Attack

No.	Type of attack	Study(s)
1	Data Injection	[7], [8], [20], [25], [27], [29], [31], [33]
2	Advance Persistence Threat	[9]
3	Switching Attack	[11]
4	Denial of Service (DOS)	[15], [19], [21], [23]
5	Distributed Denial of Service	[30]
6	Host based Attack	[16]
7	Replay Attack	[17]
8	Bias Injection	[22]
9	Random Attack	[23]
10	Cross-Site Scripting	[28]
11	General	[12], [13], [14], [18], [26], [32], [36]

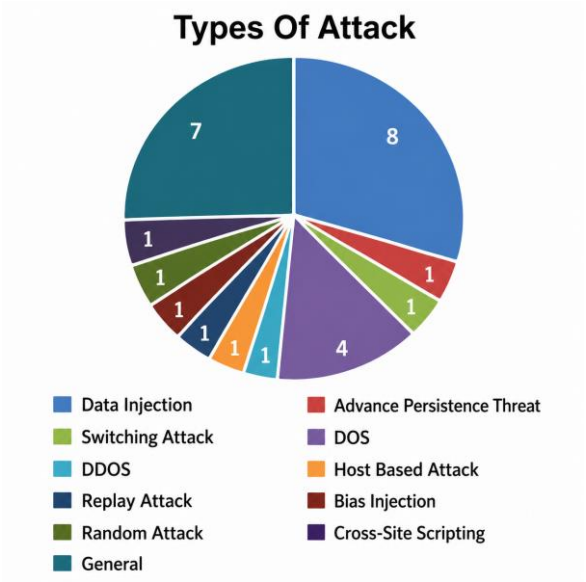

Fig. 4 Types of Attack

V. Discussion

In this section, we aimed to discover the patterns of the studies included in this SMS based on the year of publication. From Figure 5 we can see that interest in intrusion detection system is initially decreased and started to increase only after 2017. From 2018 to 2020 it shows a fluctuating pattern. This research topic reached its peak in 2021 with the number of 7 publications in that year.

https://doi.org/10.31436/ijpcc.v10i2.466

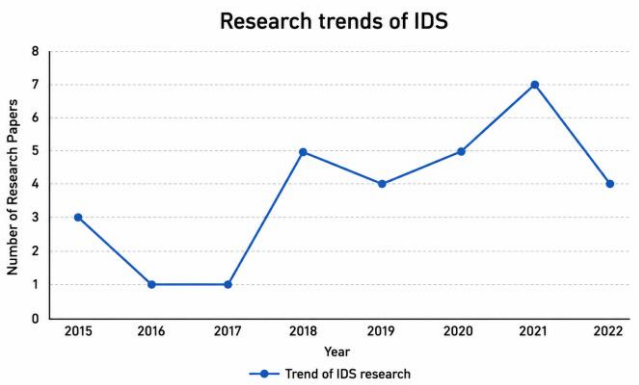

Fig. 5 Trends of IDS Research

Based on our examination of the empirical evidence we had gathered, we found that the absence of empirical evidence had a significant impact on the way we extracted data, resulting in some publications having less information presented in fewer than three pages. For this reason, a lot of data for the classification scheme is incomplete because some studies did not state them clearly. Due to the fact that a mapping study requires empirical research evidence, many of the studies retrieved from the online databases that appeared in the search results had to be disregarded. We argue that reliable findings need to be demonstrated in published studies in order to ensure selection of good quality primary studies.

VI. Conclusions

In this study, we included 30 primary studies that have been located through our SMS. This number suggests a considerably small number of studies that have been done thus far related to the intrusion detection topic. Examining the publication year, we found that this research topic has been studied since 2015.

Our research questions (RQs) assisted in the identification of issues that need to be addressed because the purpose of this study was to provide an overview of the current literature on this research topic. Through our SMS, we also learned that, in contrast to other methods, most intrusion detection system commonly used the hybrid method. The results demonstrated that Data Injection has been the primary attack type in the system on a regular basis, and this resulted in the detection of several research gaps.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

[1] M. Estifanos S. Tilahun. n.d. # Intrusion Detection System-IDS-Journal-by Sci-Tech with Estif Intrusion Detection System-IDS.

[2] A. Dou, F. Zhang, Q. Yang, and C.J. Zhang. 2022. "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures." *IEEE Transactions on Automation Science and Engineering* 19(3):1631–44. doi: 10.1109/TASE.2022.3149764.

[3] V.T. Phan, G. Loukas, Diane Gan, and A. Bezemskij. 2015. "Decision Tree-Based Detection of Denial of Service and Command Injection Attacks on Robotic Vehicles." in *2015 IEEE International Workshop on Information Forensics and Security, WIFS 2015 - Proceedings*. Institute of Electrical and Electronics Engineers Inc.

[4] W. Shimeng, Yuchen J., Hao L., and Xianling Li. 2021. "Deep Learning-Based Defense and Detection Scheme against Eavesdropping and Typical Cyber- Physical Attacks." in *2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes, SAFEPROCESS 2021*. Institute of Electrical and Electronics Engineers Inc.

[5] K. Petersen, Hochschule Fl. Robert F. Michael M. and Shahid M.. 2008. *Systematic Mapping Studies in Software Engineering*.

[6] W. Scott, and Robert S. A. n.d. The Well-Built Clinical Question: A Key to Evidence- Based Decisions. Vol. 123.

[7] M. P1 --- M. Ghaderi, K. Gheitasi and W. Lucia, "A Blended Active Detection Strategy for False Data Injection Attacks in Cyber-Physical Systems," in IEEE Transactions on Control of Network Systems, vol. 8, no. 1, pp. 168-176, March 2021

[8] J. Wei, "A data-driven cyber-physical detection and defense strategy against data integrity attacks in smart grid systems,"2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Orlando, FL, USA, 2015, pp. 667-671.

[9] J. Yang, L. Zhou, L. Wang, S. Li, Z. Lin and Z. Gu, "A Multi-step Attack Detection Framework for the Power System Network,"2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 2022, pp. 1-8.

[10] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1594-1606, Sept. 2018.

[11] J. Gao, J. Li, H. Jiang, Y. Li and H. Quan, "A new Detection Approach against attack/intrusion in Measurement and Control System with Fins protocol," 2020 Chinese Automation Congress (CAC), Shanghai, China, 2020, pp. 3691-3696.

[12] C. Zhang, D. Du, J. Zhang, M. Fei and A. Rakic, "A Novel Dynamic Watermarking-Based Attack Detection Method for Uncertain Networked Control Systems," 2021 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Shanghai, China, 2021, pp. 1- 8.

[13] A. Gorbenko, & V. Popo. Abnormal behavioral pattern detection in closed-loop robotic systems for zero-day deceptive threats. In 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) (pp. 1-6). 2020 IEEE.

[14] K. Han, S. Li, Z. Wang and X. Yang, "Actuator deception attack detection and estimation for a class of nonlinear systems," 2018 37th Chinese Control Conference (CCC), Wuhan, China, 2018, pp. 5675-5680.

[15] A. W. Al-Dabbagh, Y. Li and T. Chen, "An Intrusion Detection System for Cyber Attacks in Wireless Networked Control Systems," inIEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 8, pp. 1049-1053, Aug. 2018.

[16] T. Badgujar and P. More, "An Intrusion Detection System implementing Host based attacks using Layered Framework," 2015 International Conference on Innovations in Information, Embedded

and Communication Systems (ICIIECS), Coimbatore, India, 2015, pp. 1-4.

[17] H. Guo, Z. -H. Pang, J. Sun and J. Li, "An Output-Coding-Based Detection Scheme Against Replay Attacks in Cyber-Physical Systems," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 68, no. 10, pp. 3306-3310, Oct. 2021.

[18] B. Tulkun and B. Fayzullajon, "Analysis of Integrated Neural Network Attack Detection System and User Behavior Models," 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-4.

[19] H. Niu, C. Bhowmick and S. Jagannathan, "Attack Detection and Approximation in Nonlinear Networked Control Systems Using Neural Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 1, pp. 235-245, Jan. 2020.

[20] A. Ameli, A. Hooshyar, E. F. El-Saadany and A. M. Youssef, "Attack Detection and Identification for Automatic Generation Control Systems," in IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[21] Z. Tahir, A. Q. Khan and M. Asad, "Attack Detection and Identification in Cyber Physical Systems: An example on Three Tank System," 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2019, pp. 1-6.

[22] L. Kang and H. Shen, "Attack Detection and Mitigation for Sensor and CAN Bus Attacks in Vehicle Anti-lock Braking Systems,"2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2020, pp. 1-9.

[23] H. Li, X. He, Y. Zhang and W. Guan, "Attack Detection in Cyber- Physical Systems Using Particle Filter: An Illustration on Three-Tank System,"2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 2018, pp. 504-509.

[24] P. Ramanan, D. Li and N. Gebraeel, "Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems," inIEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 8, pp. 4727-4739, Aug. 2022.

[25] S. Tan, J. M. Guerrero, P. Xie, R. Han and J. C. Vasquez, "Brief Survey on Attack Detection Methods for Cyber-Physical Systems," in IEEE Systems Journal, vol. 14, no. 4, pp. 5329-5339, Dec. 2020.

[26] R. Anguluri, V. Katewa and F. Pasqualetti, "Centralized Versus Decentralized Detection of Attacks in Stochastic Interconnected Systems,"in IEEE Transactions on Automatic Control, vol. 65, no. 9, pp. 3903-3910, Sept. 2020.

[27] M. Xiao, J. Wu, C. Long and S. Li, "Construction of false sequence attack against PLC based power control system," 2016 35th Chinese Control Conference (CCC), Chengdu, China, 2016, pp. 10090-10095.

[28] K. Gupta, R. Ranjan Singh and M. Dixit, "Cross site scripting (XSS) attack detection using intrusion detection system,"2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 199-203.

[29] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, E. Tajik,S. Padmanaban, and H. Aliev , "Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack," in IEEE Access, vol. 9, pp. 16488-16507, 2021.

[30] A. Shi, "Cyber Attacks Detection Based on Generative Adversarial Networks," 2021 2nd Asia Conference on Computers and Communications (ACCC), Singapore, 2021, pp. 111-114.

[31] D. An, F. Zhang, Q. Yang and C. Zhang, "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures," inIEEE Transactions on Automation Science and Engineering, vol. 19, no. 3, pp. 1631-1644, July 2022.

[32] V. Krishnan and F. Pasqualetti, "Data-Driven Attack Detection for Linear Systems," in IEEE Control Systems Letters, vol. 5, no. 2, pp. 671-676, April 2021.

[33] K. Xiahou, Y. Liu and Q. H. Wu, "Decentralized Detection and Mitigation of Multiple False Data Injection Attacks in Multiarea Power Systems," in IEEE Journal of Emerging and Selected Topics in Industrial Electronics, vol. 3, no. 1, pp. 101-112, Jan. 2022.

[34] T. P. g, G. Loukas, D. Gan and A. Bezemskij, "Decision tree- based detection of denial of service and command injection attacks on robotic vehicles," 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2015, pp. 1-6.

[35] S. Wu, Y. Jiang, H. Luo and X. Li, "Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks," 2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS), Chengdu, China, 2021, pp. 1-6.

[36] H. Yang, L. Cheng and M. C. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems,"2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 2019, pp. 1-7.