International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

[1]Bhaludra R Nadh Singh, [2]Nallan Chakravarthula Sai Vyuha, [3]Mariyala Roshini
[1]Professor, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India
[2,3]Student, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

ARTICLEINFO

Article History:

Accepted: 10 June 2023
Published: 24 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
643-649

ABSTRACT

In recent years, Cyber-Physical Systems (CPSs) have attracted intense attention due to their potential applications in many areas. However, the strong reliance on communication networks makes CPSs vulnerable to intentional cyber-attacks. Therefore, a great number of attack detection methods have been proposed to enforce security of CPSs. In this paper, various false data injection attack detection methods presented for CPSs are investigated and reviewed. According to the knowledge of control information, the controllers of CPSs are categorized as centralized and distributed controllers. Existing centralized attack detection approaches are discussed in terms of (i) linear time-invariant systems, (ii) actuator and sensor attacks, (iii) nonlinear systems and (iv) systems with noise. Furthermore, the development of distributed attack detection is reviewed according to different decoupling methods. Some challenges and future research directions in the context of attack detection approaches are provided.

Index Terms: Centralized detection, cyber-attacks, cyberphysical systems, distributed detection, false data injection attack.

I. INTRODUCTION

THANKS to the rapid development of technology in communication networks, computer science and control theory, Cyber-Physical Systems (CPSs) have been extensively studied from both academia and industry. CPSs are systems that are controlled or monitored by computer-based algorithms, tightly integrated with networks and users [1], [2]. Examples of CPSs include smart grids, intelligent transportation networks, 5G cellular networks, sustainable developments, medical systems, process control systems, robotics systems and automatic pilot avionics [3]–[8].

A CPS typically consists of a network of interacting units with physical devices and computational elements [9]. The strong dependence on communication networks makes system vulnerable to cyber-attacks [10]–[12], such as Denial of Service (DoS) attacks and deception attacks [10], [13], [14]. Those attacks can be injected into systems both in cyber layer and physical layer [15]. Moreover, some malicious attackers would focus on attacks between cyber and physical layer, which can potentially induce significant damage on physical devices.

It should be noted that an attacker can either arbitrarily disturb the system dynamics or induce any perturbations to CPSs without enough security protections of hardware or software strategies, and thus leads to significant societal losses or the loss of human lives. Examples include Iranian nuclear facility struck by the Stuxnet malware, blackout accident in nuclear plant , power blackouts in Brazil, etc.

These examples indicate an urgent need for reliable attack detection schemes to deal with malicious attacks and also maintain the performance of CPSs. If cyber-attacks could be detected and located in a short time period, the damage to overall systems would be controlled within a tolerable limit. Most of the available literatures on attack detections are based on centralized architectures. As highlighted in, attack detection schemes can be often divided into knowledge-based and data-driven approaches. In most knowledge-based methods, one representative detection strategy is residual generation method. Normally, a residual is designed by comparing the measurements of the sensors with an analytical model of the system. This residual is then compared with a fixed or time various threshold in order to determine if there is an attack. It should be mentioned that the residual generation approaches are always combined with the observer-based methods or statistics analysis methods. As for data-driven methods, deep learning and heuristic algorithms are often used to build a model or map a relation of CPS. If system measurement data does not conform to some of the relationships, then an attack is assumed. Aside from the centralized systems, more and more distributed systems appears in modern life. A typical example is microgrid. A microgrid system consists of multiple energy sources, such as photovoltaic, wind turbines and batteries, which are interconnected via transmissions lines among each unit. Although these units are connected with each other, normally they are often operated independently. As a result, the distributed controllers may have limited information of the overall system dynamics. It is hard for a detector to monitor a CPS without enough information. This is the main challenge in the design of a distributed attack detection method.

In this paper, an overview of false data injection attack detection approaches for different CPS structures, methodologies and future trends is provided. A novel classification method based on the knowledge of various types of systems is provided. In this perspective, controllers for CPSs can be cat-egorized as centralized controllers and distributed controllers. Then, different attack detection methods related to these two kinds of controllers are reviewed respectively.

II. RELATED WORK

Messous and Liouane [1] presented an online successive distance vector hop scheme for node localization accuracy in WSNs. They also discussed the variation of anchor nodes with optimized distance between nodes in the network. Dong et al. [2] examined the distance vector hop algorithm against Sybil attacks for effective node localization and accuracy for improved security in WSN. The scheme also reduces the average error localization by 3%, setting the beacon nodes 50 in the simulation that is 78%. Chelouah et al. addressed localization algorithm in mobile WSNs. They also presented the mobility of nodes for coverage optimization, connectivity, and analysis. Hadir et al. presented a localization technique in WSNs using an effective distance vector hop scheme. They also discuss the average hop size and localization accuracy by exploiting the information. Almomani et al. designed a low cost and efficient, intelligent DoS attack detection and prevention technique. They also discuss different DoS attack classifications using a specialized dataset for WSN. Patel and Mistry presented Sybil node detection using various schemes. They also discussed and analyzed the protocols used in WSNs. Yavuz et al. proposed detecting IoT-routing attacks using a deep learning machine learning technique. The Cooja simulator generates high-fidelity attack data in the IoT network with 1000 sensors.

Sujatha and Anita examined the detection of Sybil attack detection using hybrid fuzzy and powerful extreme learning machines. They also discussed ARM as the main CPU with LEACH environment and ZigBee transceivers on real-time test beds. Qi et al. researched a localization algorithm to improve the node position accuracy and reducing localization error in WSNs using MA-MDS. They also use the Prussian analysis algorithm for accurate coordinate transformation. Li et al. presented a localization trust valuation scheme to detect spoofing and Sybil attacks. This scheme is obtained by selecting localization performance, estimated distance, and transmission with the threshold property set in WSNs. Song et al. proposed a chaotic hybrid mutation and chaotic inertial weight-updating technique with a glowworm swarm optimization approach. The scheme also avoids premature convergence with better convergence and higher accuracy. Saud Khan and Khan presented Sybil attack detection using signed response authentication techniques for global mobile communication systems. They also discussed the probabilistic model to analyze Sybil attack detection performance.

III. PROPOSED SYSTEM

The proposed system consists of a series of phases: design and planning, deployment and routing, data processing, training and testing, attack classification, attack detection,and localization. The data processing phase includes feature selection and normalization of the network traffic security dataset. The proposed system shown in Figure 1 is designed using optimized multilayer perceptron artificial neural network (MLPANN). The MLP is a feed-forward ANN with back propagation to calculate the gradient used for weight calculation. The ANN technique is a stochastic learning model for decision-making using interconnected information processing units. ANN can estimate the nonlinear relationship between inputs and outputs and map the exchange of information among the nodes. The multilayer perceptron (MLP), as shown in Figure 8, configured with input layers, three hidden layers, and output layers. The proposed system used a gradient descent optimization for speeding and enhancing accuracy for detection and localization of attacks. This approach also uses a statically driven technique for training and testing using multilayer perception. Several procedures are included in the proposed framework to identify malicious or unexpected routing. The method begins with a network data collection and preprocessing stage. Next, it must find any missing values in the system and then fill in those blanks with appropriate values that were not present before processing began. We use the mean as our default. Subsequently, the dataset is cleaned up by removing any occurrences of duplicate values. After that, data encoding and normalization are carried out. In order to facilitate data handling, the encoded data undergoes a dimension's reduction procedure. To aid with anomaly detection, it is necessary to do feature optimization in order to extract the most useful characteristics from the data. In order to spot outliers in the dataset, optimal feature selection is crucial. For the same information, it aids in lowering the computational cost required to process it. Below is an equation that can be used to determine the entropy.

$$E = -\sum_{i}^{L} P_i \log_2 P_i,$$

where p is the chance of finding a particular class label in the dataset. In this study, a hybrid machine learning approach is recommended for intrusion detection in a wireless sensor network after the optimal selection of features for anomaly detection.

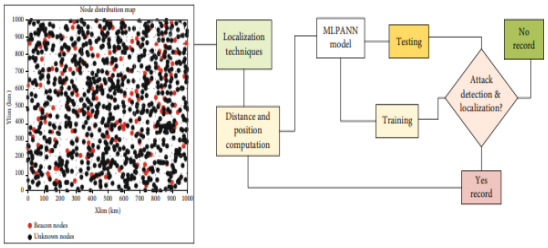

Figure 1: Secure localization techniques for detection and localization of malicious attacks using MLPANN in WSNs.

IV. IV.RESULTS AND DISCUSSION

The simulation setting configuration and evaluation metrics will be discussed in this section. Wireless sensors are distributed randomly forming clustering with cluster heads in the target field with an area of 1000 × 1000 m2. The routing protocols are used for making clustering and selection of the cluster head in each round of the simulation and localization of the unknown nodes with help of the beacon nodes and sink nodes. The cluster head achieves more computational data processing from the sensor nodes and communication with base station. The simulation parameter configuration is shown in Table 1. Intel (R) Xeon (R) Silver 4214 CPU @ 2.20GHz 2.19GHz (2 processors) with 128 GB (128 GB useable), x64-based processor, and 64-bit operating system running Windows using MATLAB R2021a is used for network planning and simulation.

Table 1: Simulation setup for the proposed network model.

Parameter	Values
Number of sensors	300-1000
Beacon nodes	60-120
Unknown nodes	240-840
Protocol type	Clustering and routing
Deployment area	$1000 \times 1000\ m^2$
Mobility	Random
Number of clusters	10
Sink position	500, 1000
Number of attacks	5-60
Data size	4000 kb
Attacks	Routing
Transmission radius	400 m

Our primary effort is devoted to determining how well various hybrid-based improvements to the original DVhop algorithm perform in detecting and pinpointing hostile nodes that have hijacked the beacon node and are supplying false routing information. All of our proposed algorithms have been implemented in the MATLAB simulator for thorough testing and analysis of their localization faults and precision. Numerous researchers rely on MATLAB, a simulation programed and numerical computing environment, to test out new ideas, conduct research, and build models. In our tests, we have examined the localization accuracy and the localization error per node by changing the percentage of anchor nodes, the total number of sensor nodes, and the nodes' communication range across four different topologies. One way to measure an algorithm's efficacy in localization is by looking at how it performs on average with regard to localization errors. We employ IBM SPSS, Python, and the WEKA Java toolboxes for data processing and analysis to gauge the effectiveness of the suggested strategy against the dataset. The average error of localization to all the nodes is calculated using Equation. The clustering and routing protocols are used for clustering and selection of the cluster head selection and maximizing the network lifetime and improving the network performance.

The routing attacks including the sinkhole attacks, blackhole attacks, and Sybil attacks are used in the simulation scenario for evaluating the localization and detection accuracy. The simulation results depict that the data processed from the environment is authenticated and registered.

Figure 2 shows data processing and aggregation by the cluster head sent to the base station (BS). Figures 2(a) and 2(b) show the dynamic clustering and data retrieval of the sensors by the beacon nodes. The cluster head (CH) aggregates huge message size as in Figures 2(c) and 2(d); the sensor nodes (SNs) consume greater time form data execution. Registration phases are utilized to identify sensor nodes, aggregation nodes, and base stations using smart contact of the public blockchain. The intelligent communications verify the existence of the aggregation node validated by its MAC address and its identity checked by the base station. The public blockchain records of validated aggregated nodes and stored data of the aggregated node provide reliable authentication techniques in WSNs. The sensor nodes are allowed to join the blockchain after the completion of the registration process to reduce external attacks on WSNs.

The sensor nodes have aggregation nodes after random deployment in the target field. The aggregation nodes authenticate the identities of the sensor nodes using a private for communicating with them, and the base station also authenticates the aggregation node for communicating with it using a public key. The aggregation nodes communicate with each other using mutual authentication process. Figure 3 shows the distribution and the experimental simulation of the nodes. Moreover, this work introduces the average localization error and coverage, localization, and detection accuracy as evaluation metrics. The average localization error (ALE), average localization accuracy (ALA), accuracy, detection rate precision, and recall are used as evaluation metrics. The average error localization, shortened as ALE [2], is computed as follows in Equation.

The ALE is the summation of the LE of all the unknown nodes to the total number of unknown nodes. The LE is the difference between estimated and actual position of unknown nodes.

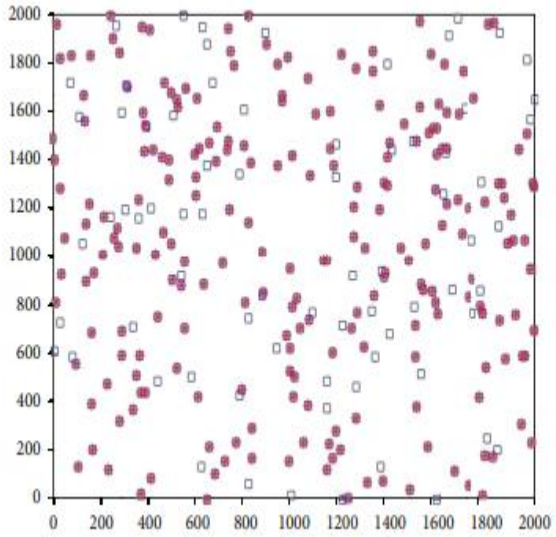

Fig 2 (a) Beacon node distribution phases

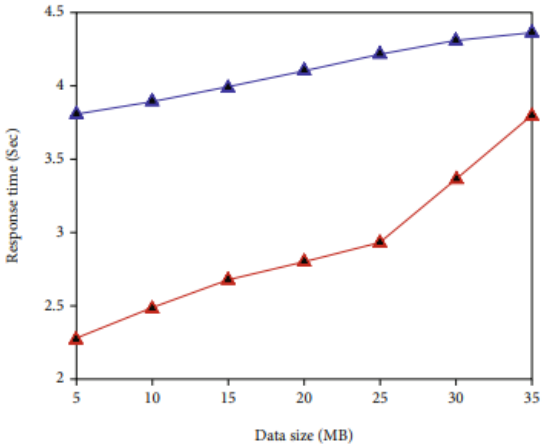

Fig 2 (b) Data uploading and retrieval phases

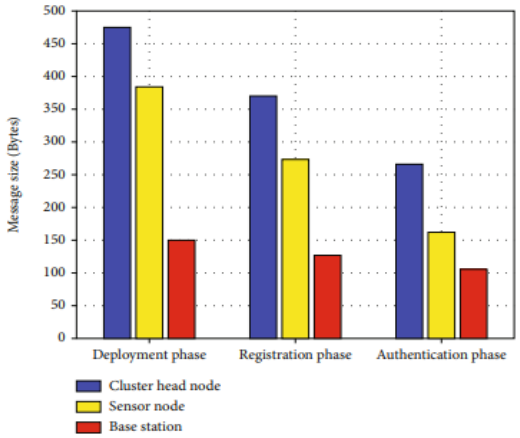

Fig 2(c) Authentication and registration phases in SN, CH, and BS

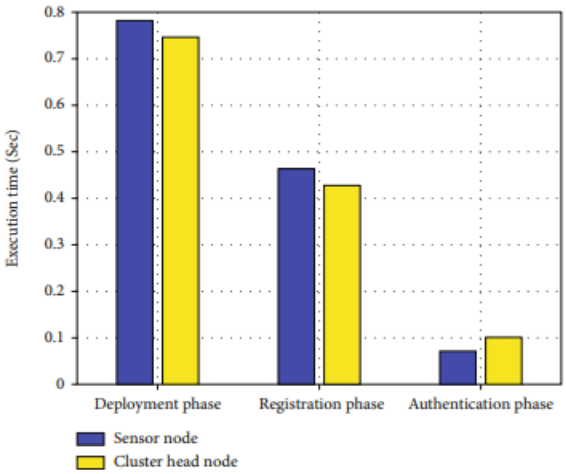

Fig 2(d) Authentication and registration phases in SN and CH

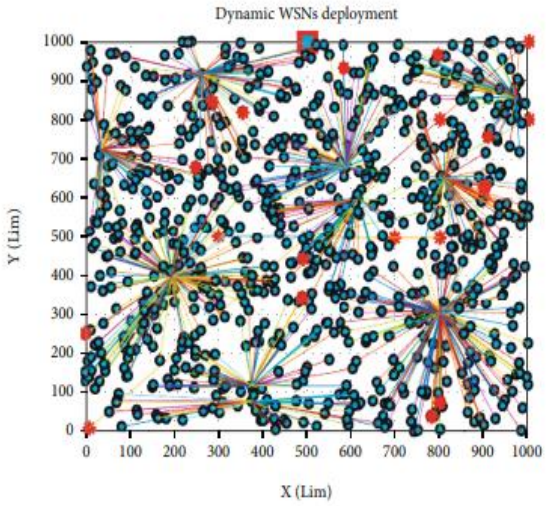

Fig 3(a) Clustering and localization of WSNs

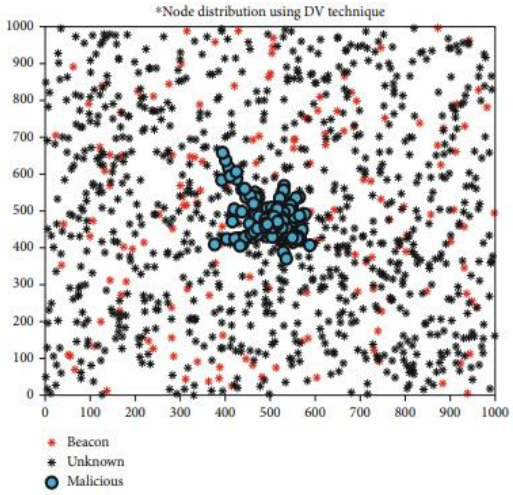

Fig 3 (b) Malicious node localization in WSNs

V. CONCLUSION

In this work, we proposed a multilayer perception artificial neural network (MLPANN) for detecting and localizing multiple attacks in WSNs. The proposed scheme achieved an average detection accuracy of 100%, 99.65%, 98.95%, and 99.83% for the various malicious nodes using UNSWNB, WSN-DS, NSL-KDD, and CICIDS2018 benchmark datasets, respectively. The optimized localization approach is more effective and performs more significantly by 20% than the distance vector hop technique, with average localization accuracy of 99.12% using 160 beacon nodes. The validation of the proposed method is confirmed with the previous studies using the ANN classification technique using Python, IBM SPSS, and WEKA toolboxes for data processing and MATLAB R2021a for network planning and simulation. The datasets are used to evaluate the proposed system for detecting and localization accuracy of different attacks. The effectiveness of the proposed scheme is assessed using detection rate, ROC, false-positive rate, a lifetime of the network, residual energy, and the area under the curve metrics. The beacon, sensor, and malicious nodes were used hierarchically to simulate the target field. It is recommended to enhance further the detection and localization of accuracy of malicious nodes using different approaches in WSNs. We will extend this work with various attack classes and methods. The results show that performance and security of the proposed scheme are applicable for scalable and large network coverage in wireless sensor networks with heterogeneous and homogenous sensors for ensuring quality of services and availably. The proposed scheme will be examined in the future using other network planning and tools with different public datasets as benchmarks for detecting and localization attacks in WSNs.

VI. REFERENCES

[1]. S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid,” Proceedings of the IEEE, vol.100, no. 1, pp. 210–224, 2011.

[2]. C. Murguia, N. van de Wouw, and J. Ruths, “Reachable sets of hidden cps sensor attacks: Analysis and synthesis tools,” IFAC-PapersOnLine,vol. 50, no. 1, pp. 2088–2094, 2017.

[3]. H. Chen, “Applications of cyber-physical system: a literature review,”Journal of Industrial Integration and Management, vol. 2, no. 03, p.1750012, 2017.

[4]. Y. Lu, “Cyber physical system (cps)-based industry 4.0: a survey,”Journal of Industrial Integration and Management, vol. 2, no. 03, p.1750014, 2017.

[5]. S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," IEEE Systems Journal, vol. 9, no. 2, pp. 350–365, 2014.

[6]. R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyberphysical communication in 5g cellular networks: challenges, spatial spectrum sensing, and cyber-security," IET Cyber-Physical Systems: Theory & Applications, vol. 2, no. 1, pp. 49–54, 2017.

[7]. J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: stateof-the-art, needs and perspectives," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2389–2406, 2018.

[8]. R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, "Big data meet cyber-physical systems: A panoramic survey," IEEE Access, vol. 6, pp.73 603–73 636, 2018.

[9]. E. A. Lee, "Cyber physical systems: Design challenges," in 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). IEEE, 2008, pp. 363–369.

[10]. C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," IEEE Transactions on Systems, Man, and Cybernetics: Systems,2019.

[11]. M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," Neurocomputing, 2019.

[12]. H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic control, vol. 59, no. 6, pp. 1454–1467, 2014.

[13]. A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," Automatica,vol. 51, pp. 135–148, 2015.

[14]. A. Teixeira, D. Perez, H. Sandberg, and K. H. Johansson, "Attack ´models and scenarios for networked control systems," in Proceedings of the 1st international conference on High Confidence Networked Systems. ACM, 2012, pp. 55–64.

[15]. H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in 2012 IEEE 51st IEEE Conference on Decision and Control (CDC). IEEE, 2012, pp. 3412–3417.

Cite this article as :

Bhaludra R Nadh Singh, Nallan Chakravarthula Sai Vyuha, Mariyala Roshini, "Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 3, pp. 643-649, May-June 2023.

Journal URL : https://ijsrset.com/IJSRSET23103156