ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-17***

CYBERATTACK DETECTION IN DYNAMIC HIERARCHICAL POWER DISTRIBUTION SYSTEMS

[#1]K.SAVITHA, ***Assistant Professor,***
[#2]K.RAVI, ***Assistant Professor,***
Department of Computer Science & Engineering,
Mother Theressa College of Engineering & Technology, Peddapalli, Telangana.

ABSTRACT: The potential uses of cyber-physical systems, or CPSs, across a wide range of industries have attracted a lot of attention recently. Because of their reliance on communication networks, CPSs are susceptible to malicious intrusions. To ensure the safety of CPS, several attack detection techniques have been developed. This research looks at different ways that CPSs can be attacked with fake data injection and compares them. Centralized or distributed CPS controllers are defined by the level of understanding of control information. I present centralized attack detection methods are tested on linear time-invariant systems, (ii) sensor and actuator attacks, (iii) nonlinear systems, and (iv) systems influenced by noise. In addition, a wide variety of decoupling procedures are employed to research the evolution of dispersed assault detection. We talk about certain limitations and possible future research areas in the area of attack detection systems.

Indexterms: Centralized detection, cyber-attacks, cyber physical systems, distributed detection, false data injection attack.

1. INTRODUCTION

The fast development of computer science, information networks, and control theory has led to a great deal of research on Cyber-Physical Systems (CPSs) in both academic and industrial contexts. In computerized control and monitoring systems, there is a strong relationship between users and networks. A few examples of cyber-physical systems (CPSs) are smart utilities, smart transportation networks, 5G cellular networks, medical systems, robotics systems, autonomous pilot avionics, process control systems, and sustainable upgrades.

Common components of cyber-physical systems (CPSs) include interconnected mechanical and electrical devices. Dependence on communication networks—which are vulnerable to hacking techniques like denial-of-service (DoS) and deception attacks—is a big issue with the system. A device's software and hardware are both vulnerable to these types of assaults. Bad actors may potentially use the intersection of physical and cyber levels as a vulnerability to cause significant harm to technology. An attacker can cause a lot of problems in cyber-physical systems (CPSs) if the software or hardware doesn't have enough security mechanisms to stop it. Society as a whole might feel the personal and financial repercussions of this. Nuclear power plant blackouts and the Stuxnet virus's impact on Iran and Brazil are just two examples.

This highlights the significance of having solid threat monitoring strategies to deter fraudsters and guarantee the smooth operation of CPS. The system could be protected from harm if hackers could be located and tracked down faster. The vast majority of materials pertaining to

DOI: https://doi.org/10.5281/zenodo.19017122

assault detection focus on solitary, centralized systems. Systems that rely on expert knowledge and those that rely on hard data are the two main categories of threat monitoring tools. When looking for representations, the majority of knowledge-based systems use the residual generation method. Comparing sensor data with an analytical model of the system is one approach to finding residuals. Next, the residual value is compared to a threshold that is either predetermined or changes over time to determine if an assault has occurred. Keep in mind that methods to generate residuals are frequently used in conjunction with statistical or observer-based analytic methodologies. To create a model or map of the interplay between cyber and physical systems (CPS), data-driven approaches frequently use heuristic algorithms and deep learning. System data that deviates from typical patterns may indicate an attack is taking place. Centralized and decentralized technologies are both widely used nowadays. This is most exemplified by a microgrid. Microgrids are networks of interconnected transmission lines that link consumers to distributed generation resources including solar panels, wind turbines, and batteries. Although these components are interdependent, they frequently possess distinct vigor. This means that managers in various locations might not have a complete picture of the system. Inadequate data makes it hard to monitor a Cyber-Physical System (CPS). Developing a strategy to detect spread attacks is fraught with difficulty.

The frequency, methods, and consequences of fake data injection attacks on different Cyber-Physical System (CPS) designs are investigated in this article. Based on our knowledge of different systems, we present a new approach to classification. We differentiate between CPS control strategies that are centralized and those that are decentralized. Subsequently, various methods for detecting assaults on both types of controllers are outlined.

2. LITERATURE SURVEY

An improved method for precisely arranging nodes in Wireless Sensor Networks (WSN) was proposed by Messous and Liouane (year). Their strategy includes making use of a sequential distance vector hop device that is accessible online. With an emphasis on optimally dividing up network nodes, the authors also discussed the evolution of anchor nodes. In order to prevent Sybil attacks in WSNs, Dong et al. used the distance vector hop technique to improve the accuracy and precision of node positions. Adding 50 beacon nodes reduces the average localization error in the simulation by 78%.

Mobile wireless sensor networks (WSNs) were the primary focus of the research by Chelouah et al. The researchers also proved that optimization in coverage, communication, and analysis is improved by node mobility. Using a distance vector hop method, Hadir et al. discovered an excellent approach to pinpointing the locations of WSNs. Additionally, we examine the data to learn more on the typical amount of hops and the precision of the location.

The approach to detecting and preventing DoS assaults developed by Almomani et al. is cutting-edge, inexpensive, and effective. Using a dataset developed for WSNs, the authors also examine several types of DoS assaults. Patel and Mistry used many approaches to identify Sybil nodes in their research. The researchers also examined and assessed the

protocols used by Wireless Sensor Networks (WSNs).

Deep learning machine learning techniques can be used to identify vulnerabilities in IoT routing, according to Yavuz et al. Using a network of one thousand sensors, the Cooja simulator generates comprehensive and realistic attack data on an IoT network. According to Sujatha and Anita's findings, a combination of fuzzy learning and strong extreme learning machines is the most effective method for detecting Sybil attacks. Other topics covered by the writers include the operation of ZigBee transceivers on real-time test platforms and the inner workings of the CPU in the LEACH (Low-Energy Adaptive Clustering Hierarchy) system.

Specifically, Qi et al. investigated MA-MDS, a localization approach for WSNs, to improve node positioning accuracy and decrease localization errors. To double-check the coordinate transformation, the Prussian analysis method is also employed. An approach to localization based on trust values was developed by Li et al. to detect deceit and Sybil attacks. This approach makes use of the threshold feature and the fact that WSNs can precisely determine their location, distance, and data relay capabilities. Song et al. introduced a novel approach to improving glowworm swarm optimization by combining a chaotic hybrid mutation strategy with a chaotic inertial weight-updating method. It prevents convergence from happening too soon and makes it happen faster and more correctly; the technique does double duty in this regard. Researchers Saud Khan and Khan devised a method to detect Sybil attacks in WSNs as part of their investigation. Such processes are identified using signed response authentication mechanisms. The authors also touched on the topic of using a probabilistic technique to assess how well Sybil attack detection works.

3. RELATED WORK

The steps of the proposed system include design and planning, routing and deployment, data processing, training and testing, attack classification, detection, and location. Data processing for security datasets related to network traffic requires the selection and standardization of specific attributes.

The device sports a multilayer perceptual artificial neural network, as seen in Figure 1. One feed-forward artificial neural network (ANN) that uses the gradient from backpropagation to update the network's weights is the multilayer perceptron, or MLP. One probabilistic model of learning is the Artificial Neural Network (ANN) technique, which uses a network of interconnected computer nodes to analyze data and make judgments. Numerous applications exist for artificial neural networks (ANNs), including accurately depicting the flow of data between interconnected nodes and determining the non-linear correlation between input and output variables. As shown in Figure 8, a Multilayer Perceptron (MLP) consists of three layers: one for inputs, one for outputs, and one for hidden layers. The presented technique employs gradient descent optimization to enhance the accuracy and speed of attack detection and localization.

A new approach based on a constant is used to teach and test multilayer perception. Several methods to detect and prevent improper or unusual routing are part of the architecture design under consideration. As a first step, you must collect and organize all the relevant network

DOI: https://doi.org/10.5281/zenodo.19017122

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-17***

data. The next step is for the system to restore any missing values that were not there before processing by checking for them. Compromise is always within our reach. Displaying the dataset follows the removal of duplicates. Once it is done, data standardization and decoding can commence. Data that has had the number of its dimensions reduced can be more easily handled using this method. Anomaly detection becomes much simpler using feature optimization, which entails selecting the most pertinent data elements.

The most important part of learning to detect outliers in a dataset is picking the right attributes. Computer processing of the same quantity of data is cheaper. By plugging the values into the formula, you may determine the entropy of any given system.

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

The probability of finding a specific label within a given category is represented by the letter p. This research aimed to fill a gap in the literature by developing a hybrid machine learning method for WSN intrusion detection. The key to success with this approach is settling on reliable criteria for identifying extreme cases.

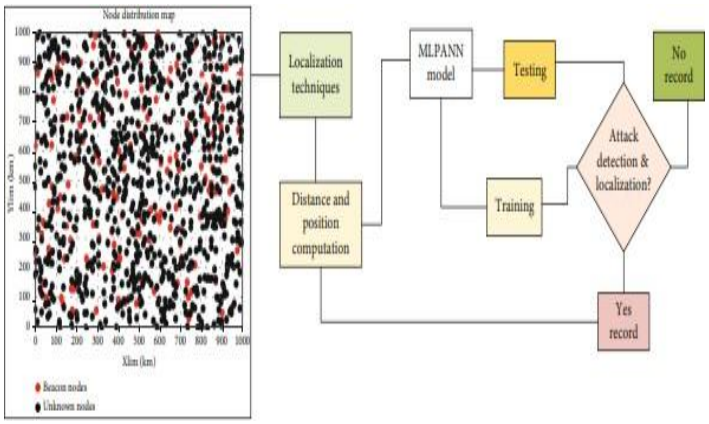

Figure 1: Secure localization techniques for detectionand localization of malicious attacks using MLPANNinWSNs.

4. RESULTS AND DISCUSSION

The steps for running a simulation and analyzing its output are detailed here. A million square meters of dispersed wireless sensors will cluster around a leader node. Each modeling iteration begins with the routing protocols forming groups of nodes and selecting a group leader. Additionally, you can use sink and beacon nodes to locate undiscovered nodes. Data is transmitted from sensor nodes to the hub by the cluster leader. Table 1 displays the parameters used in the simulation. The 64-bit Windows system that we use to run MATLAB R2021a is powered by an Intel Xeon Silver 4214 CPU, which is capable of 2.20GHz (2 processors) and 1.19GHz (with 128GB of accessible RAM).

Table 1: Simulation setup for the proposed networkmodel.

DOI: https://doi.org/10.5281/zenodo.19017122

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

The primary goal of our research is to evaluate the effectiveness of several hybrid-based improvements to the original DVhop algorithm in identifying and locating rogue nodes that have displaced the beacon node and are transmitting erroneous routing information. All of our approaches have been thoroughly tested for accuracy and faults in localization using the MATLAB simulator. Numerous scientists rely on MATLAB, a numerical computing environment that is both simulation-programmed and generalized, to conduct experiments, compile data, and build models. By varying the total number of sensor nodes, the communication range of the nodes, and the number of anchor nodes, we investigated the accuracy and variability of localization error across four separate configurations. In this scenario, the average number of localization errors produced by the algorithm is a good indicator of its performance. To test the efficacy of the suggested approach on the dataset, we process and analyze the data using Python, IBM SPSS, and the WEKA Java toolboxes. The average distance between any two nodes can be determined using the above equation. By assisting with activities such as creating and selecting clusters and their leaders, routing and clustering algorithms can improve the performance and lifespan of networks.

The effectiveness of localization and detection is evaluated in the simulated environment through the use of Sybil attacks, sinkhole attacks, and blackhole assaults. According to the simulation results, the environmental data that was provided and accepted is accurate.

Data is collected and organized by the cluster head before being sent to the BS, as shown in Figure 2. Both 2(a) and 2(b) depict the sensor data collection and dynamic clustering processes that occur among the beacon nodes. The sensor nodes (SNs) need more time to process data, as shown in Figure 2(d), while the cluster head (CH) receives more messages, as shown in Figure 2(c). During the registration process, the public blockchain's smart contact is used to locate base stations, aggregation nodes, and sensor nodes. To verify the identity and presence of the aggregation node, the base station use its Media Access Control (MAC) address. There is a great deal of confidence in authentication procedures used by WSNs because the public blockchain records all authenticated aggregated nodes and the data stored on them. Weaknesses in WSN security can be mitigated by registering sensor nodes on the blockchain.

Sensors are dispersed around the target region and linked by aggregation nodes once they have been located. In order to verify the identity of the sensor nodes, the nodes that aggregate data use a private key. In contrast, the aggregating node's identity is verified by the base

station using a public key. A system of aggregating nodes is established by mutual authentication. Figure 3 shows the node count and a sample run of the simulation. To aid in performance evaluation, the average localization error is now one of the available indicators. Accuracy in localization, recognition rate, and coverage are also part of this list. As metrics for assessment, we make use of recall, average localization error (ALE), precision of the detection rate, accuracy, and average localization accuracy (ALA). The average error localization (ALE) can be determined using an equation ([2,]).

The LE of a total unknown node is added to the total number of unknown nodes to obtain the ALE. The LE reveals the degree to which a node deviates from its ideal position.

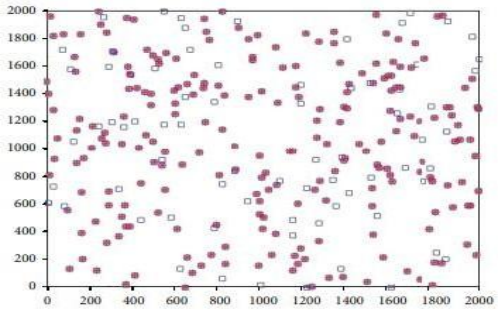

Fig2 (a)Beacon nodedistributionphases

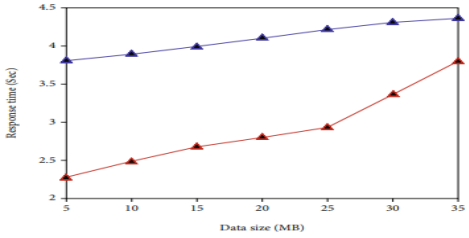

Fig2(b)Datauploadingand retrievalphases

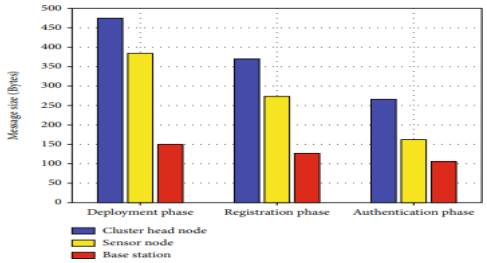

Fig 2(c) Authentication and registration phases inSN, CH, and BS

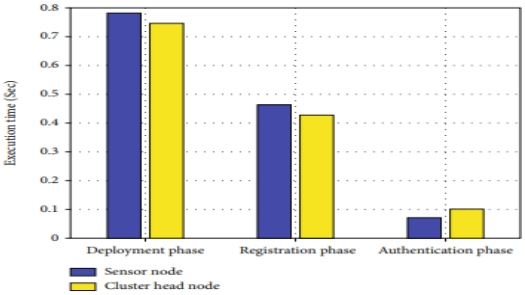

Fig 2(d) Authentication and registration phases in SN and CH

DOI: https://doi.org/10.5281/zenodo.19017122

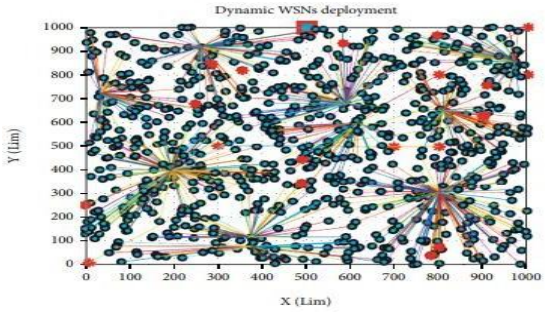

Fig3(a)Clustering and localization ofWSNs

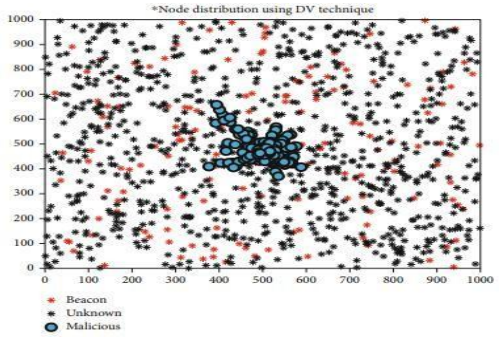

Fig3(b) Maliciousnodelocalization inWSNs

5. CONCLUSION

The approach to precisely locate an attack in a Wireless Sensor Network (WSN) using a Multi-Layer Perceptron Artificial Neural Network (MLPANN) is demonstrated in this research. Using the UNSWNB, WSN-DS, NSL-KDD, and CICIDS2018 standard datasets, the suggested technique was evaluated. With respect to individual cancer nodes, the average detection accuracies were as follows: 100%, 99.65%, 98.95%, and 99.83%. The distance vector hop method is 20% less effective than the optimum localization strategy.

Localization accuracy with 160 beacon nodes averages 99.12%. Previous research have proven that the suggested approach works using ANN classification using MATLAB R2021a for network construction and simulation and Python, IBM SPSS, and WEKA toolboxes for data analysis. The datasets are used to evaluate the proposed system's attack detection and identification capabilities.

The proposed system is evaluated by detection rate, ROC, false positive rate, residual energy, area under the curve, network lifetime, and residual energy. We created our ecosystem by hierarchizing beacons, sensors, and bad nodes. Malicious WSN nodes can be found in numerous methods. Program communities and attacks will grow. The findings show that the suggested method's security and performance are crucial to the continuous availability and high quality of a large-scale, scalable WSN network with homogenous and heterogeneous sensors. We will evaluate the WSN attack detection and prevention method using public datasets, network designs, and technologies.

REFERENCES

[1].S.Sridhar,A.Hahn,andM.Govindarasu,“Cyber–physical system security for the

electricpower grid," Proceedings of the IEEE, vol.100,no. 1, pp.210–224, 2011.
[2].C.Murguia,N.vande Wouw,andJ.Ruths,"Reachablesetsofhiddencpssensorattacks:Analysisandsynthesistools,"IFAC-PapersOnLine,vol.50,no.1,pp.2088–2094,2017.
[3].H.Chen,"Applicationsofcyber-physicalsystem: a literature review,"Journal of IndustrialIntegrationandManagement,vol.2,no.03,p.1750012,2017.
[4].Y.Lu,"Cyberphysicalsystem(cps)-basedindustry4.0:asurvey,"JournalofIndustrialIntegrationandManagement,vol.2,no.03,p.1750014,2017.
[5].S.K.KhaitanandJ.D.McCalley,"Designtechniquesandapplicationsofcyberphysicalsystems: Asurvey,"IEEESystemsJournal,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 5gcellular networks: challenges, spatial spectrumsensing,andcyber-security,"IETCyber-PhysicalSystems: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 technologiesfor sustainable development goals: stateof-the-art,needsandperspectives,"IEEECommunications Surveys & Tutorials, vol. 20,no.3, pp.2389–2406, 2018.
[8].R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang,"Bigdatameetcyber-physicalsystems:Apanoramic survey," IEEE Access, vol. 6, pp.73603–73 636, 2018.
[9].E.A.Lee,"Cyberphysicalsystems:Designchallenges,"in200811thIEEEInternationalSymposiumonObjectandComponent-OrientedReal-TimeDistributedComputing(ISORC).IEEE, 2008, pp.363–369.
[10].C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "Asurvey on security communication and controlfor smart grids under malicious cyber attacks,"IEEETransactionsonSystems,Man,andCybernetics:Systems,2019.
[11].M.S.Mahmoud,M.M.Hamdan,andU.A.Baroudi,"Modelingandcontrolofcyber-physicalsystemssubjecttocyberattacks:Asurveyofrecentadvancesandchallenges,"Neurocomputing,2019.
[12].H. Fawzi, P. Tabuada, and S. Diggavi, "Secureestimationandcontrolforcyber-physicalsystemsunderadversarialattacks,"IEEETransactions on Automatic control, vol. 59, no.6, pp. 1454–1467,2014.
[13].A. Teixeira, I. Shames, H. Sandberg, and K. H.Johansson,"Asecurecontrolframeworkforresource-limitedadversaries,"Automatica,vol.51, pp. 135–148, 2015.
[14].A. Teixeira, D. Perez, H. Sandberg, and K. H.Johansson,"Attack´models andscenariosfornetworked control systems," in Proceedings ofthe1stinternationalconferenceonHighConfidenceNetworkedSystems.ACM,2012,pp.55–64.
[15].H. Fawzi, P. Tabuada, and S. Diggavi, "Securityfor control systems under sensor and actuatorattacks," in 2012 IEEE 51st IEEE Conference onDecision and Control (CDC). IEEE,2012, pp.3412–3417.