DETECTION OF CYBERATTACKS IN DYNAMIC, HIERARCHICAL DISTRIBUTION SYSTEMS

#1ANARAJULA REKHA,
#2Dr.P.VENKATESHWARLU, ***Associate Professor,***
#3Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: Cyber-Physical Systems (CPSs) have received a great deal of attention in recent years due to their potential applications in a wide range of industries. CPSs are vulnerable to intentional cyber-attacks due to their reliance on communication networks. As a result, in order to assure CPS security, numerous attack detection mechanisms have been created. This research examines and compares various methods for detecting spurious data injection attacks on CPSs. The comprehension of control information dictates whether CPS controllers are centralized or dispersed. Using (i) linear time-invariant systems, (ii) actuator and sensor assaults, (iii) nonlinear systems, and (iv) noise-affected systems, the effectiveness of existing centralized attack detection algorithms is evaluated. Furthermore, the evolution of distributed attack detection is investigated by employing various decoupling mechanisms. Some limitations and future research potential in the realm of assault detection techniques are discussed.

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

1. INTRODUCTION

As a result of the rapid development of information networks, computer science, and control theory, Cyber-Physical Systems (CPSs) have been the subject of much study in both academic and industrial settings. The users and networks are tightly intertwined in CPSs, which stands for computerized control and monitoring systems. Smart utilities, intelligent transportation networks, 5G cellular networks, sustainable developments, medical systems, process control systems, robotics systems, and autonomous pilot avionics are all examples of Cyber-Physical Systems (CPSs).

A Cyber-Physical System (CPS) is often a collection of interconnected electronic and mechanical devices. The system's dependence on communication networks is a major weakness that can be exploited by hacking techniques including denial of service (DoS) and deception attacks. Both the digital and physical components of a system are vulnerable to these kinds of attacks. The intersection of the cyber and physical levels is also a potential weak spot that malicious actors may exploit to cause extensive harm to hardware. An attacker can cause havoc in cyber-physical systems (CPSs) if there aren't sufficient security mechanisms in the hardware or software to prevent it. This can have severe financial and human consequences for society. Power outages at nuclear plants, as well as those in Brazil and Iran due to the Stuxnet computer virus, are just a few examples.

All of this highlights the urgent necessity for effective attack monitoring techniques to thwart cybercriminals and guarantee the smooth operation of CPS. Damage to the system as a whole might be mitigated if hackers could be detected and followed more rapidly. The vast majority of resources devoted to the topic of attack detection focus on single, centralized infrastructures. Knowledge-based systems and data-driven systems are the two primary categories into which threat monitoring tools fall. The residual generation method is commonly utilized in most knowledge-based systems as a means of locating representations. Residuals are often calculated by comparing sensor data to an analytical model of the system. The presence or absence of an assault is then determined by comparing the residual value to a predetermined or time-dependent threshold. Remember that residual generating techniques are frequently used with statistical or observer-based analysis techniques. In data-driven approaches, a model or map of the connection between cyber and physical systems (CPS) is commonly constructed using deep learning and heuristic algorithms. When data from the system is inconsistent with expected patterns, an attack is suspected. Today, it's not uncommon to find both centralized and decentralized forms of technology in use. The best example of this is the concept of a microgrid. Transmission lines comprise a microgrid system, which links renewable energy generators like solar panels, wind turbines, and batteries to consumers. Despite their interconnected nature, each of these factors often exerts its own force. Thus, it is conceivable for managers in various locations to have only a partial grasp of the system as a whole. Lack of information makes it difficult to monitor a Cyber-Physical System (CPS). The primary difficulty in developing a strategy for locating spread attacks is the core task itself.

This research explores the prevalence of false data injection attacks across a variety of Cyber-Physical System (CPS) architectures, as well as their mechanisms and potential outcomes. We propose a new classification scheme based on our understanding of various systems. Here, we distinguish between centralized and decentralized control strategies for complex physical systems (CPS). Following this, several techniques for spotting attacks on either variety of controller are discussed.

2. LITERATURE SURVEY

Messous and Liouane (year) developed a novel method for improving the precision of node placement in Wireless Sensor Networks (WSN). An online sequential distance vector hop device is implemented as part of their plan. The authors also discussed the evolution of anchor nodes, with special attention paid to the optimal separation of network nodes. Dong et al. conducted research on how to prevent Sybil assaults in wireless sensor networks (WSNs) by using the distance vector hop technique to increase node accuracy and location precision. In the simulation, adding 50 beacon nodes results in a significant 78% reduction in the average localization error.

Mobile wireless sensor networks (WSNs) were the subject of research conducted by Chelouah et al. The researchers also demonstrated how the mobility of the nodes contributes to the enhancement of optimization across the board, including coverage, communication, and analysis. Hadir et al. demonstrated a highly efficient position determination method for WSNs based on a distance vector hop technique. The data is also analyzed to learn more about the typical number of hops and the precision of location.

The method developed by Almomani et al. to detect and halt Denial of Service (DoS) attacks is low-cost, effective, and technologically advanced. The authors also use a dataset created specifically for Wireless Sensor Networks (WSNs) to analyze various forms of DoS assaults. In their study, Patel and Mistry considered a variety of techniques for locating Sybil nodes. The researchers also carefully examined and assessed the Wireless Sensor Network (WSN) protocols.

To detect IoT-routing threats, Yavuz et al. propose using deep learning machine learning techniques. The Cooja simulator generates realistic and comprehensive attack data on an IoT network using a network of one thousand sensors. In their research, Sujatha and Anita found that a combination of mixed fuzzy and powerful extreme learning machines is most effective at detecting Sybil attacks. The authors also discussed the employment of ZigBee transceivers on real-time test platforms and the central processor unit (CPU)'s role in the LEACH (Low-Energy Adaptive Clustering Hierarchy) system.

Qi et al. looked at a localization technique called Multi-Agent Multi-Dimensional Scaling (MA-MDS), which was developed to enhance node positioning precision and decrease localization errors in WSNs. Coordinate transformation is checked using the Prussian analysis method as well. Li et al. developed a trust value approach for localization to detect dishonesty and Sybil attacks. The success of Wireless Sensor Networks (WSNs) in determining their position, making distance estimates, and transmitting data is combined with the threshold property to create this method. In their research, Song et al. developed a novel approach to enhancing glowworm swarm optimization by combining a chaotic hybrid mutation strategy with a chaotic inertial weight-updating method. The strategy not only prevents convergence from occurring prematurely, but also accelerates it and improves its accuracy. In their research, Saud Khan and Khan developed a methodology for detecting Sybil assaults in wireless data networks. To locate such procedures, signed response authentication strategies are employed. The authors also discussed the use of a probabilistic approach to evaluate Sybil attack detection effectiveness.

3. RELATED WORK

Design and planning, deployment and routing, data processing, training and testing, attack classification, attack detection, and localisation are all crucial components of the proposed system's stages. Processing data for network traffic security datasets involves selecting and standardizing characteristics. In Figure 1, we can see the device's MLPANN (multilayer perception artificial neural network). In order to update the network's weights based on the gradient calculated by the backpropagation technique, the Multilayer Perceptron (MLP) is a feed-forward ANN. The Artificial Neural Network (ANN) technique is a probabilistic model of learning that makes use of interconnected computational nodes to analyze data and draw conclusions. Accurately mapping the flow of information between linked nodes and determining the non-linear correlation between input and output variables are two of the many uses for artificial neural networks (ANNs). A Multilayer Perceptron (MLP) has the structure seen in Figure 8: three hidden layers, three input layers, and three output layers. The demonstrated solution employs gradient descent optimization to boost attack recognition and localization throughput and precision.

Another mechanism driven by a constant is used to teach and evaluate multilayer perception in this approach. The under study architecture design includes a number of mechanisms for detecting and blocking abnormal or malicious routing. The first step is to gather necessary network data and prepare it for use. The system must then check for missing values and restore them if they were not there prior to processing. We always settle for the middle option. After that, duplicates are removed and the dataset is made presentable. After that, data decoding and standardization can begin. To make it more manageable, encoded data undergoes a dimension reduction process. Anomaly recognition can be improved through feature optimization, which involves selecting the most relevant aspects of the data. Choosing the correct features is the most crucial step in learning how to identify outliers in a dataset. The cost of using computers to process the same volume of data decreases. The entropy of a system can be calculated using the provided equation.

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

The probability of locating a given category label is denoted by the symbol p. The purpose of this research was to propose a hybrid machine learning approach to intrusion detection in a WSN. This method centers on how to pick attributes that are optimal for spotting outliers.

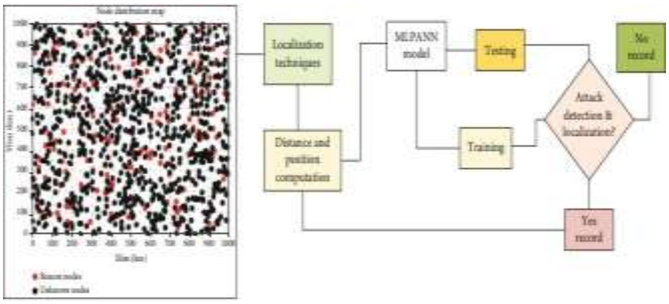
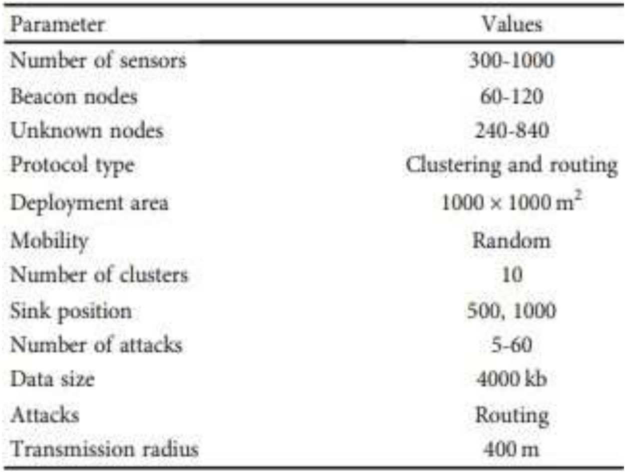


Figure 1: Secure localization techniques for detection and localization of malicious attacks using MLPANNin WSNs.

4. RESULTS AND DISCUSSION

Here, we'll discuss the steps involved in preparing a simulation and doing an analysis of its results. When wireless sensors are dispersed at random across a 1,000,000-square-meter field, clusters form with leaders. The routing protocols are used to form clusters of nodes and select a leader for each cluster at the beginning of each modeling iteration. Using beacon and sink nodes, they can also be utilized to locate previously undiscovered nodes. The leader of the cluster receives information from the sensor nodes and relays it to the hub. The simulation's parameters can be seen in Table 1. We use a 64-bit Windows installation with MATLAB R2021a on an Intel Xeon Silver 4214 CPU running at 2.20GHz (2 processors) and 1.19GHz (with 128GB of usable memory).

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	$1000 \times 1000\ \text{m}^2$
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 focus is on testing various hybrid-based enhancements to the original DVhop algorithm in their ability to detect and pinpoint malicious nodes that have gained control of the beacon node and are broadcasting erroneous route information. Our approaches have all been thoroughly examined for errors and localization precision using the MATLAB simulator. Many scientists utilize MATLAB, a simulation-programmed and numerical computing environment, to test out hypotheses, collect data, and build models. We examined the precision and variation in localization error across four distinct designs by varying the number of anchor nodes, the total number of sensor nodes, and the nodes' communication range. Examining the typical number of localization errors made by the algorithm can provide insight into its efficacy in this area. We process and analyze the data using IBM SPSS, Python, and the WEKA Java toolboxes to see how well the suggested technique performs on the dataset. The equation is used to calculate the mean distance between every pair of nodes. Networks can be optimized for performance and longevity through the use of clustering and routing techniques for tasks such as creating and selecting clusters and their respective leaders.

Sinkhole attacks, blackhole attacks, and Sybil assaults are used to test how well localization and detection work in the simulated scenario. The simulation's findings confirm that environmental data has been verified and recorded.

As can be seen in Figure 2, the cluster head collects and processes information before sending it on to the BS. The dynamic clustering and data collection from sensors by beacon nodes is depicted in Figures 2(a) and 2(b). The cluster head (CH) in Figure 2(c) receives more messages, whereas the sensor nodes (SNs) in Figure 2(d) process data more slowly. In order to locate sensor nodes, aggregation nodes, and base stations during the registration process, smart contact of the public blockchain is utilized. Using its Media Access Control (MAC) address, the base station verifies the existence of the aggregation node and its identity. Because the public blockchain keeps track of verified aggregated nodes and the data held on the aggregated nodes, WSNs can use authentication mechanisms with high levels of confidence. Registering sensor nodes on the blockchain makes WSNs more resistant to external attacks.

The sensors are dispersed around the area of interest and connected via aggregation nodes once they have been found. The aggregating nodes check the names of the sensor nodes against a private key. In contrast, the base station relies on a public key to authenticate the aggregating node. Through mutual authentication, the aggregation nodes form a network. The number of nodes and a test run of the simulation are displayed in Figure 3. In order to better evaluate performance, the average localization error has been added alongside coverage, localization accuracy, and recognition rate. We employ the average localization error (ALE), the average localization accuracy (ALA), the accuracy, the precision of the detection rate, and the recall as assessment metrics. The average error localization (ALE) is calculated using an equation ([2,]).

A total unknown node's LE is added to the total number of unknown nodes to get the ALE. The LE represents the discrepancy between a node's predicted and observed location.

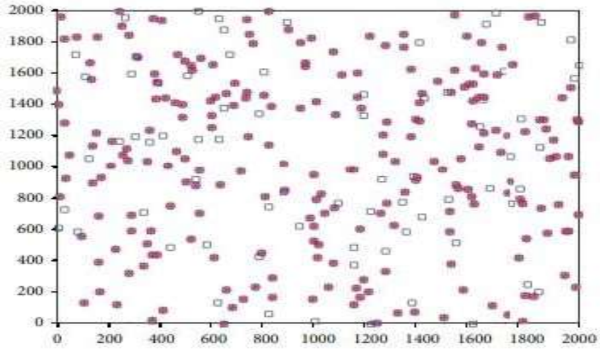


Fig 2 (a) Beacon node distribution phases

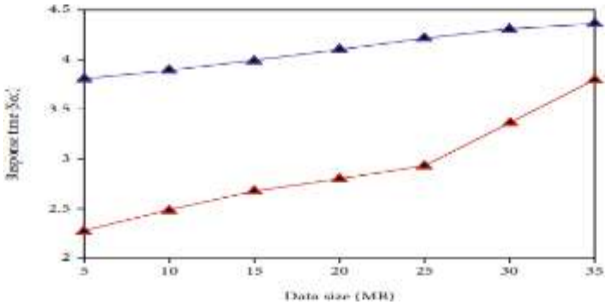


Fig 2 (b) Data uploading and retrieval phases

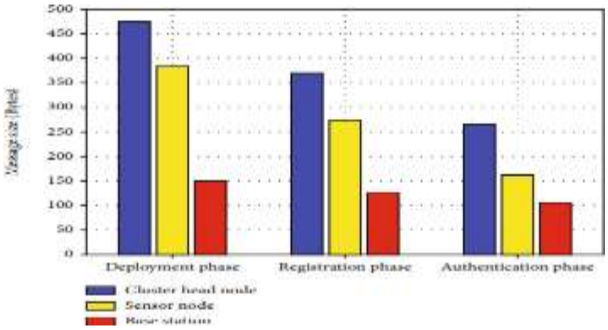


Fig 2(c) Authentication and registration phases in SN, CH, and BS

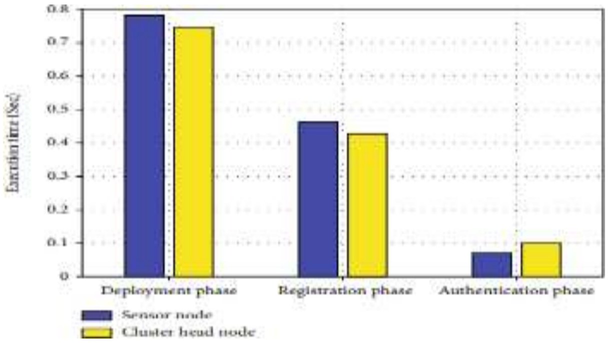


Fig 2(d) Authentication and registration phases in SN and CH

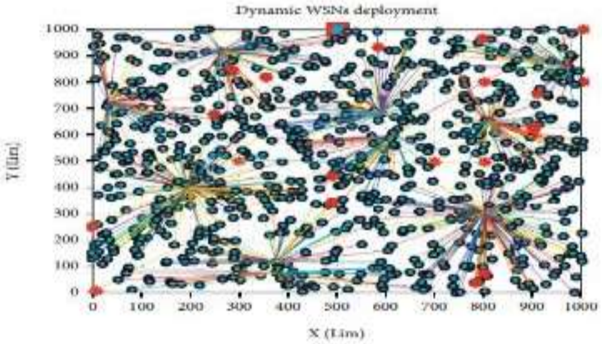


Fig 3(a) Clustering and localization of WSNs

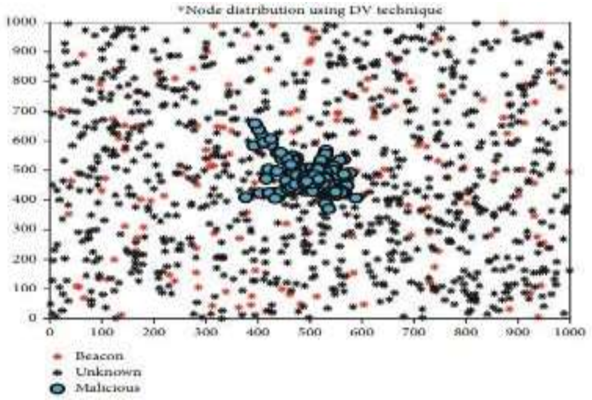


Fig 3 (b) Malicious node localization in WSNs

5. CONCLUSION

In this work, we present the use of an MLPANN to identify the precise location of an assault in a WSN. Average detection accuracies for various malignant nodes using the proposed technique were 100%, 99.65%, 98.95%, and 99.83% when tested on the UNSWNB, WSN-DS, NSL-KDD, and CICIDS2018 standard datasets, respectively. When compared to the distance vector hop approach, the optimized localization method is 20% more efficient. The average localization accuracy is 99.12 percent when 160 beacon nodes are used. The effectiveness of the suggested method has been demonstrated by prior research employing the ANN classification technique with Python, IBM SPSS, and WEKA toolboxes for data processing and MATLAB R2021a for network construction and simulation. To see how successfully the proposed system can detect and localize various forms of attacks, it is put to the test on the provided datasets. The detection rate, ROC, false positive rate, network lifetime, residual energy, and area under the curve are used to evaluate the proposed system's efficacy. Hierarchies of beacon, sensor, and malicious nodes were constructed to simulate the sought-after environment. Different approaches are proposed to make it simpler to locate and detect rogue nodes in WSNs. More communities and assault strategies will be incorporated into this program. Results demonstrate the significance of the proposed scheme's performance and security in ensuring service quality and availability across a vast and scalable network of heterogeneous and homogeneous sensors in wireless sensor networks. The effectiveness of the proposed method in detecting and localizing assaults in WSNs will be evaluated against alternative network designs and technologies, as well as various publicly available datasets.

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.