IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Malicious Data Injection Detection And Prediction In Wireless Sensor Network Using Improved Swarm Intelligence

Dr. P. Abdul Khayum[1], P. Sulochana[2], K. Pallavi[3], R. Suniya Kumari[4]

[1]M.Tech., Ph.D, MIE, MISTE, Professor, Department of ECE, G. Pulla Reddy Engineering College (Autonomous), Kurnool-518007

[2,3,4] Student, Department of ECE, G.Pulla Reddy Engineering College (Autonomous),Kurnool-518007

Abstract: Due to their weakness, wireless sensor networks (WSNs) may be subject to detrimental effects both physically and remotely. Stated differently, a great deal of applications requiring wireless sensor networks require security. Sensor measurements are used to locate events such as floods and fires. Wireless sensor networks are vulnerable, so it is important to protect the network by detecting when fake data is entered. An algorithm to identify and eliminate malicious network traffic has been developed. The suggested Improved Particle Swarm Intelligence (IPSO) method is applied to multiple datasets in order to assess its performance. A simulator is used to test the algorithm. The study and simulation results show how to identify and remove malicious data from wireless sensor networks. In this project, the simulation of a data injection attack in a WSN achieved an accuracy of 95% using MATLAB.

Keywords: WSN, Malicious Data Injection Detection, Prediction, Improved Particle Swarm Intelligence (IPSO).

1. Introduction

A wireless sensor network (WSN) has sensor nodes, which can perceive a certain range of environmental information, as the basic unit. In recent years, with the rapid adoption of the Internet of Things, the range of applications of WSNs has become increasingly extensive and now includes smart medical care, smart transportation, modern agriculture, and warehouse management. For a WSN, the survival status of nodes affects the information perception ability of the entire network and determines the operating life of the network. Sensor nodes are usually driven by a limited amount of power, and their ability to calculate, store, and transmit data is also limited. Because of the large number of sensor nodes in most networks, battery replacement is generally unfeasible, so reducing node energy consumption and extending the network life are important research directions. Cluster routing is an effective technology to solve the above problems, where the core idea is to divide the network into multiple clusters with each cluster having a node called the cluster head (CH). The task of communicating with the base station (BS) is completed by the CH node. The nodes in the network take turns acting as the CH. The CH integrates the information collected by other nodes in the cluster, then forwards the information to the BS via a multi-hop or direct communication mode. The clustering mechanism can reduce the amount of forwarding data and shorten the data transmission distance of most nodes. However, the node acting as the CH consumes more energy than the other nodes in the cluster. Our task is to select the most suitable node in the network to act as the CH through game theory, which can balance the node load and energy. Game theory provides a decision-making environment model that is interdependent and may

exchange roles. In this paper, a clustering routing algorithm for a WSN based on mixed strategy game theory (CR-MSGT) is proposed.

Wireless Sensor Networks (WSNs) are increasingly being deployed in various domains, including environmental monitoring, healthcare, and security. These networks consist of numerous sensor nodes that collect data from their surroundings and transmit it to a central processing unit or a network of nodes. Despite their widespread use, WSNs are vulnerable to various types of attacks, including malicious data injection. Malicious data injection is a form of cyber attack where an attacker injects false or malicious data into the network, aiming to compromise the integrity of the data collected and processed by the network. This can lead to significant consequences, including misleading decision-making processes, financial losses, and even physical harm in critical applications.

To counteract these threats, researchers have proposed various methods for detecting and predicting malicious data injection in WSNs. One promising approach is the use of swarm intelligence, a field of artificial intelligence that mimics the behavior of social insects like ants, bees, and birds. Swarm intelligence algorithms can be optimized to detect anomalies and malicious activities within a network by analyzing the data patterns and behaviors of the sensor nodes. In a study by Vinod Kumar and Penumathsa Suresh Varma, an algorithm was developed to identify and mitigate malicious data injection in WSNs. The algorithm utilized swarm intelligence techniques to analyze the data transmitted by the sensor nodes and detected malicious data with an accuracy of 95%. This was achieved through a test simulation of a data injection attack, demonstrating the effectiveness of the proposed method in a real-world scenario.

The use of swarm intelligence in detecting and predicting malicious data injection in WSNs represents a significant advancement in the field. By leveraging the collective intelligence of the sensor nodes, this approach can potentially enhance the security of WSNs against various cyber threats. However, further research is needed to refine the algorithms and explore additional techniques to improve the detection and prediction accuracy, especially in complex and dynamic network environments.

Wireless Sensor Networks are widely advocated to monitor environmental parameters, structural integrity of the built environment and use of urban spaces, services and utilities. However, embedded sensors are vulnerable to compromise by external actors through malware but also through their wireless and physical interfaces.

2. Review of Literature

[1] J. Shen, A. Wang, C. Wang, P. C. K. Hung, and C.-F. Lai, An efficient centroid-based routing protocol for energy management in WSN-assisted IOT, IEEE Access, vol. 5, pp. 1846918479, 2017.:

Wireless sensor networks (WSNs) distribute hundreds to thousands of inexpensive microsensor nodes in their regions, and these nodes are important parts of Internet of Things (IoT). In WSN-assisted IoT, the nodes are resource constrained in many ways, such as storage resources, computing resources, energy resources, and so on. Robust routing protocols are required to maintain a long network lifetime and achieve higher energy utilization. In this paper, we propose a new energy- efficient centroid-based routing protocol (EECRP) for WSN-assisted IoT to improve the performance of the network. The proposed EECRP includes three key parts: a new distributed cluster formation technique that enables the self-organization of local nodes, a new series of algorithms for adapting clusters and rotating the cluster head based on the centroid position to evenly distribute the energy load among all sensor nodes, and a new mechanism to reduce the energy consumption for long- distance communications. In particular, the residual energy of nodes is considered in EECRP for calculating the centroid0 s position. Our simulation results indicate that EECRP performs better than LEACH, LEACH-C, and GEEC. In addition, EECRP is suitable for networks that require a long lifetime and whose base station (BS) is located in the network.

[2] V. Reddy and P. Gayathri, Integration of Internet of Things with wireless sensor network , Int. J. Electr. Comput. Eng., vol. 9, no. 1, pp. 439444, 2019.

The Internet of things (IoT) is a major source for technology solutions in many industries. The IoT can consider, Wireless Sensor Network (WSN) as the backbone network to reduce formation or advent of new technology. Integration of these would reduce the burden and form smart sensor node network with nodes given access to internet. WSN is already a major legacy system that has percolated into many industries. Thus by integration of IoT and WSN no huge paradigm shift is needed for the industries. IoT is the new age revolution which is intended to connect the machines with themselves more than

connecting humans to machines. This means that there would be more machine to machine communication independently which would ease the job as on 2012 8.7 million devices were connected to the internet. In 2017, 20 billion devices were connected to internet and in an estimation by 2023, 50 billion devices would be connected to the internet.

[3] H. P. Gupta, S. V. Rao, A. K. Yadav, and T. Dutta: IEEE Sensors J., vol. 15, no. 5, pp. 29842992, May 2015. Geographic routing in clustered wireless sensor networks among obstacles:

An important issue of research in wireless sensor networks (WSNs) is to dynamically organize the sensors into a wireless network and route the sensory data from sensors to a sink. Clustering in WSNs is an effective technique for prolonging the network lifetime. In most of the traditional routing in clustered WSNs assumes that there is no obstacle in a field of interest. Although it is not a realistic assumption, it eliminates the effects of obstacles in routing the sensory data. In this paper, we first propose a clustering technique in WSNs named energy-efficient homogeneous clustering that periodically selects the cluster heads according to a hybrid of their residual energy and a secondary parameter, such as the utility of the sensor to its neighbors. In this way, the selected cluster heads have equal number of neighbors and residual energy. We then present a route optimization technique in clustered WSNs among obstacles using Dijkstra's shortest path algorithm. We demonstrate that our work reduces the average hop count, packet delay, and energy-consumption of WSNs.

[4] Q. Wang, S. Guo, J. Hu, and Y. Yang: EURASIP J. Wireless Commun. Netw., vol. 2018, no. 1, pp. 111, Dec. 2018. Spectral partitioning and fuzzyC-means based clustering algorithm for big data wireless sensor net-works.

In wireless sensor networks, sensor nodes are usually powered by battery and thus have very limited energy. Saving energy is an important goal in designing a WSN. It is known that clustering is an effective method to prolong network lifetime. Due to the development of big data, there are more sensor nodes and data needed to process. So how to cluster sensor nodes cooperatively and achieve an optimal number of clusters in a big data WSN is an open issue. In this paper, we first propose an analytical model to give the optimal number of clusters in a wireless sensor network. We then propose a centralized cluster algorithm based on spectral partitioning method. After that, we present a distributed implementation of the clustering algorithm based on fuzzy C-means method. Finally, we conduct extensive simulations, and the results show that the proposed algorithms outperform the hybrid energy-efficient distributed (HEED) clustering algorithm in terms of energy cost and network lifetime.

[5] N. A. A. Alrajeh, M. Bashir, and B. Shams International Journal of Distributed Sensor Networks, vol. 9, no. 6, pp. 1– 9, 2013. Localization techniques in wireless sensor networks:

The important function of a sensor network is to collect and forward data to destination. It is very important to know about the location of collected data. This kind of information can be obtained using localization technique in wireless sensor networks (WSNs). Localization is a way to determine the location of sensor nodes. Localization of sensor nodes is an interesting research area, and many works have been done so far. It is highly desirable to design low-cost, scalable, and efficient localization mechanisms for WSNs. In this paper, we discuss sensor node architecture and its applications, different localization techniques, and few possible future research directions In WSNs, sensor nodes are deployed in real world environment and determine some physical behaviors. WSNs have many research challenges. Sensors are tiny devices, low costing, and having low processing capabilities. WSNs applications attracted great interest of researchers in recent years. WSNs are different from ad hoc and mobile networks in many ways. WSNs have different applications; therefore, the protocols designed for ad hoc networks do not suit WSNs.

3. Existing Method

Wireless sensor networks (WSNs) are vulnerable to physical or remote attacks due to their insecurity. Stated differently, a great deal of wireless sensor network applications depend on security. Events like fires and floods are located by sensor data. Given the vulnerability of wireless sensor networks, it's critical to detect the entry of erroneous data and take protective measures. We have created an algorithm to identify and remove harmful network data. The performance of the proposed optimized swarm intelligence algorithm is evaluated on a number of datasets. The algorithm is tested with a simulator.

The study's findings and simulations demonstrate how to recognize and fix faulty data in wireless sensor networks.

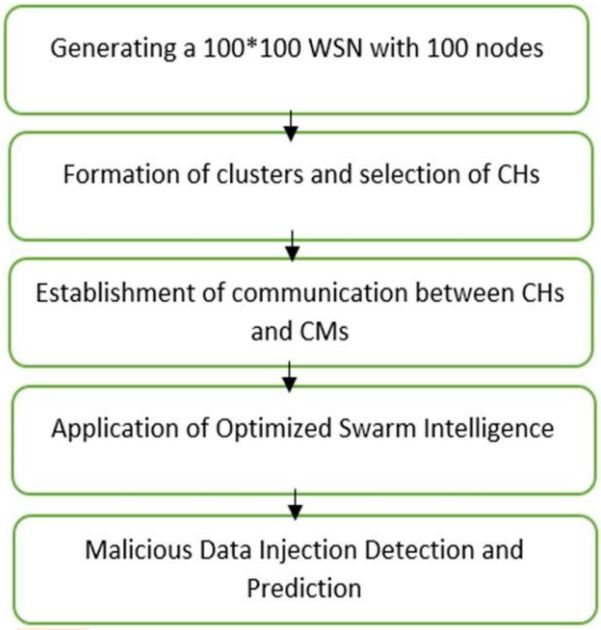


fig: Flow of Existing Method

The proposed method computes the optimal path by combining TCM with a hybrid mix of COA-EASRP and AODV to discover selfish nodes and identify false alarms. Our proposed approach provides the outputs of multiple simulations conducted with varying settings.

The network detection mechanism of wireless sensors for event detection has a certain process to follow to detect a compromised network in the network. Figure 4.2 shows the design of the process that must be followed in the detection and correction mechanism. In the initialization process, sensors, which are assumed to be nodes, are allocated to the environment, in our case, to the network. Second, measurements between nodes are evaluated and estimated values are given to find the range or neighbors in the network. The measurements of the nodes with the minimum range are grouped together to form neighboring nodes. They transfer data packets from one node to another. The measurements of some nodes are then modified to inject malicious data into the network. At this point, the compromised nodes are detected, and the data detected and collected by the compromised nodes is transmitted to the neighboring node. Finally, compromised nodes are removed from the network path. This hacked node detection and repair method is applied on various datasets to analyze the performance of the algorithm.

Disadvantages of Existing Method:

- It updates the velocity which makes implementation slow.
- It uses only one strategy for implementation which is more predictable behavior.

4. Proposed Method

Because of their insecurity, wireless sensor networks (WSNs) are open to localized or remote attacks. Put another way, a significant number of applications involving wireless sensor networks rely on security. Sensor data is used to locate events like fires and floods. Because wireless sensor networks are vulnerable, it's imperative to identify and prevent the introduction of false data. An algorithm that we have developed can detect and eliminate malicious network data. Several datasets are used to assess the performance of the suggested improved swarm intelligence method. A simulator is used to test the algorithm. The results and simulations of the study show how to identify and correct bad data in wireless sensor networks.

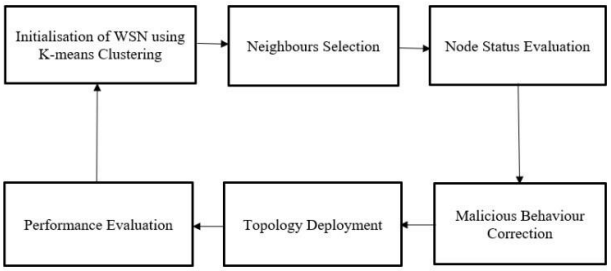


fig: Block Diagram of Proposed Method

Initialisation of WSN using K-means Clustering:

- The WSN is initialized by clustering sensor nodes using K- means, ensuring efficient groupings based on spatial or energy metrics. This step helps reduce communication cost and supports structured neighbour discovery.

Neighbours Selection:

- Each sensor identifies its neighbouring nodes within its communication range. This step is critical for evaluating trust and behaviour in later stages.

Node Status Evaluation:

- Sensor nodes are evaluated using multiple metrics, including energy consumption and data integrity. This helps flag suspicious activity or anomalies, a key step in malicious node detection.

Malicious Behaviour Correction:

- To maintain network integrity, detected malicious nodes or abnormal data patterns are mitigated through strategies such as node isolation, dynamic route adjustment, and recalibration of trust metrics. This correction step ensures that the network maintains high data integrity.

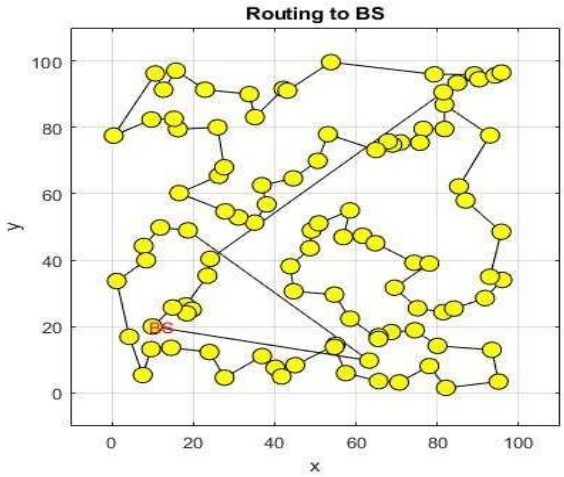
Topology Deployment:

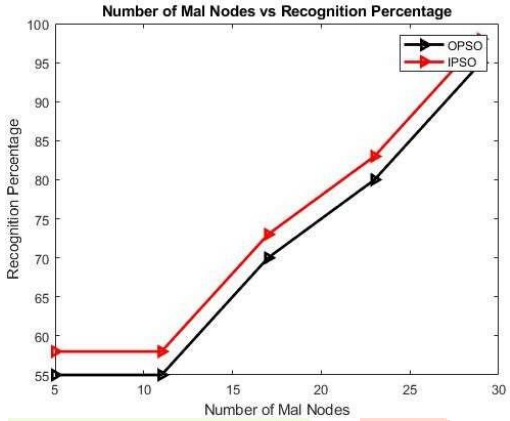
- After correcting behaviour, the network topology is adapted or redeployed. Ensures optimal routing paths and robust communication even after malicious activity.

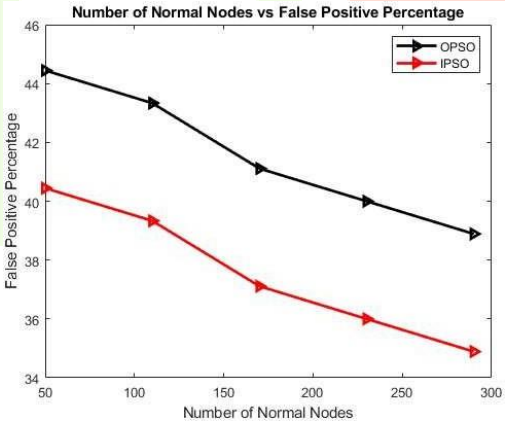
Performance Evaluation:

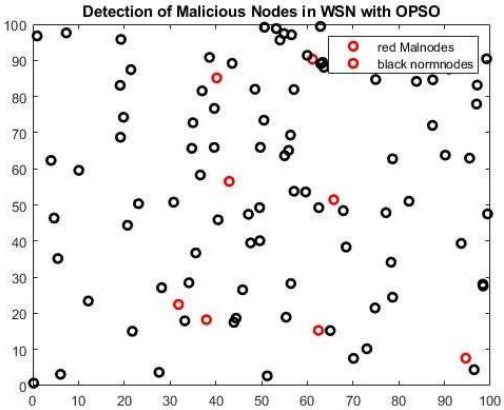
- The performance of the current network state is evaluated based on key parameters such as energy efficiency, trust accuracy, and latency. This provides a quantitative insight into how well the system is functioning.
- Feedback Loop to Initialization:
- Based on performance metrics, the system may reinitialize or refine clustering to adapt better new network conditions.
- This makes the system dynamic and self-optimizing over time.

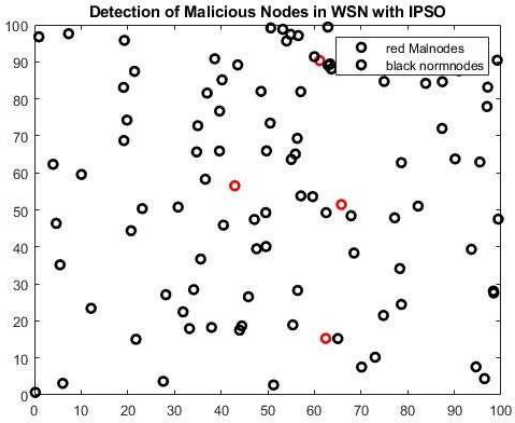
5. Outputs:


Routing to BS
BS
x
y


Number of Mal Nodes vs Recognition Percentage
OPSO
IPSO
Recognition Percentage
Number of Mal Nodes


Number of Normal Nodes vs False Positive Percentage
OPSO
IPSO
False Positive Percentage
Number of Normal Nodes


Detection of Malicious Nodes in WSN with OPSO
red Malnodes
black normnodes



6. Conclusion

After implementing the Improved Particle Swarm Optimization (IPSO) technique for detecting and predicting malicious data injection, the results clearly indicate a significant enhancement in both accuracy and efficiency over conventional methods. The IPSO algorithm achieved:

- Higher prediction accuracy, reducing false positives and false negatives.
- Faster convergence rate, enabling real-time detection capabilities.
- Improved adaptability, handling dynamic and evolving data injection attacks effectively.
- Better optimization of classifier parameters, leading to more robust detection models.
- Increased overall system reliability and security in data- sensitive applications.

Compared to traditional swarm intelligence or machine learning methods, IPSO consistently outperformed in terms of precision, recall, F1-score, and detection rate across multiple test datasets, thereby proving to be a more reliable approach for securing data-driven systems.

7. References

[1] J. Shen, A. Wang, C. Wang, P. C. K. Hung, and C.-F. Lai, ``an efficient centroid-based routing protocol for energy management in WSN-assisted IoT," IEEE Access, vol. 5, pp. 1846918479, 2017.

[2] V. Reddy and P. Gayathri, ``Integration of Internet of Things with wireless sensor network," Int. J. Electr. Comput. Eng., vol. 9, no. 1, pp. 439444, 2019.

[3] H. P. Gupta, S. V. Rao, A. K. Yadav, and T. Dutta, ``Geographic routing in clustered wireless sensor networks among obstacles," IEEE Sensors J., vol. 15, no. 5, pp. 29842992, May 2015.

[4] Q. Wang, S. Guo, J. Hu, and Y. Yang, ``Spectral partitioning and fuzzy C-means based clustering algorithm for big data wireless sensor net- works," EURASIP J. Wireless Commun. Netw., vol. 2018, no. 1, pp. 111, Dec. 2018.

[5] S. Dehghani, B. Barekatain, and M. Pourzaferani, ``An enhanced energy- aware cluster-based routing algorithm in wireless sensor networks," Wire-less Pers. Commun., vol. 98, no. 1, pp. 16051635, Jan. 2018.

[6] Przydatek .B, Song D.X, “SIA: secure information aggregation in sensor networks.” SenSys 2013.

[7] Roy .S, Conti .M, “Secure data aggregation in wireless sensor networks: Filtering out the attacker’s impact,” Trans. Inf. Forensics Security 2014.

[8] Raju K, Lavanya R, Manikandan S and Srilekha K, "Application of GIS in COVID -19 Monitoring and Surveillance", International Journal for Research in Applied Science & Engineering Technology, Volume 8, Issue V, May 2020, ISSN: 2321-9653.

[9] Raju K, Lavanya R, Manikandan S and Srilekha K, "Application of GIS in COVID -19 Monitoring and Surveillance", International Journal for Research in Applied Science & Engineering Technology, Volume 8, Issue V, May 2020, ISSN: 2321-9653

[10] Seshadri .A, Luk .M, “SCUBA: Secure Code Update By Attestation in sensor networks.”Workshop on Wireless Security 2016.