International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Malicious Data Injection Detection and Prediction in Wireless Sensor Network Using Improved Swarm Intelligence

Throvagunta Srinija[1], Potnuru Asrith[1], Dandu Mohan Pavan Satyanarayana Raju[1], Bora Balaji Basanth[1], Krishnardhula Pavan Kumar[2]

B.TECH Student, Department of Computer Science and Engineering [CSO], Raghu Engineering College, Visakhapatnam, India[1]

M.TECH [Ph. D] and Guide, Department of Computer Science and Engineering [CSO], Raghu Engineering College, Visakhapatnam, India[2]

ARTICLEINFO

Article History:

Accepted: 25 March 2024
Published: 12 April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
608-619

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's 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 swarm intelligence 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.

Keywords: WSN, Malicious Data Injection Detection, Prediction, Improved Swarm Intelligence.

I. INTRODUCTION

Wireless sensor networks are widely supported for monitoring environmental parameters, the built environment's structural integrity, and the utilization of services, utilities, and metropolitan areas.

However, because of their physical and wireless interfaces, embedded sensors can be compromised by other parties via malware. It is possible to manipulate compromised sensors to report erroneous data in an effort to elicit unsuitable and maybe harmful reactions. Because these malicious data injections can mimic realistic sensor behavior, including failures or the detection of events that never happen, they can be especially challenging to identify in cases where numerous sensors have been hijacked. This assessment examines previous research on malicious data injection in wireless sensor networks, identifies broad guidelines and categorizes methods used in this field, contrasts previous findings, and When several

sensors are compromised, this vulnerability is worsened since compromised sensors can mimic realistic sensor activity, making it more challenging to identify malicious data injections.

The detection and prediction of malicious data injections in WSNs are critical to maintaining the integrity and reliability of sensor data. Traditional methods of detection often struggle to identify malicious data injections, especially in scenarios involving multiple colluding sensors. This is where swarm intelligence, inspired by the collective behavior of social insects, presents a promising approach. Swarm intelligence algorithms can be optimized to detect anomalies and predict malicious activities in WSNs more effectively than traditional methods.

The use of improved swarm intelligence in WSNs involves developing algorithms that leverage the collective intelligence of the network to identify and mitigate malicious data injections. These algorithms can analyze sensor data in real-time, identify patterns that deviate from normal behavior, and predict potential malicious activities. By doing so, they can enhance the security and reliability of WSNs, ensuring that the data collected is accurate and trustworthy.

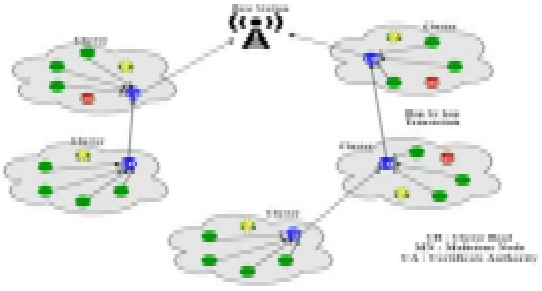

Figure 1: Clustered Wireless Sensor Environment with Malevolent Node: Sensor nodes, lightweight procedures, and data optimization are used to create a highly distributed wireless sensor network. Wireless sensor networks using sink, sensor node values, base station characteristics, and Internet of Things enabled services may monitor variables like as heat, water level, pressure, and others.

Each sensory information is recorded in the base station and controls the network in each hop-by-hop. Aggregation is another factor to find network lifetime and traffic characteristics. Many schemes have been proposed to mitigate these problems, but only a few can effectively and correctly detect the severity of the network. Many researchers analyzed various literatures in terms of network topology, attack capabilities, critical capabilities, limitations, endurance, and robustness levels. Efficiency is another factor in the WSN environment and provides a better way to detect attacks.

Among other things, wireless sensor networks (WSNs) are being utilized more often to monitor different environmental indicators and structure integrity. These networks do, however, have serious security issues, mainly from hostile nodes that may jeopardize the accuracy of the data gathered and may have negative effects. The functioning and security of a WSN environment are seriously threatened by the existence of malicious nodes, particularly when those nodes are a member of a cluster.

Malicious nodes can be detected and managed through various techniques, including neighbor-based detection methods, secure data aggregation protocols, and distributed trust models. These methods aim to identify and mitigate the risks posed by malicious nodes, ensuring the reliability and security of the data collected by the network.

One approach to detecting malicious nodes is through neighbor-based detection, as discussed by Yim and Choi in 2012. This method involves analyzing the behavior of a node's neighbors to identify any anomalies that could indicate malicious activity. This approach is particularly effective in networks where nodes are closely connected, allowing for a more detailed analysis of each node's behavior.

Secure data aggregation techniques are another critical component in managing malicious nodes within WSNs. Gomathi, Yalini, and Revathi proposed

a secure data aggregation technique that aims to protect the network from security threats, including those posed by malicious nodes. This technique involves the use of a certificate authority (CA) to authenticate nodes and ensure that only trusted nodes can participate in data aggregation. This method enhances the security of data aggregation by preventing malicious nodes from injecting false data into the network .

The security against cooperative attacks by malicious nodes is a major difficulty in WSNs. To counter such attacks, Chang et al. suggested a cooperative bait detection strategy.

This method involves using a bait node to attract malicious nodes, which can then be identified and isolated from the network. This approach is particularly effective in networks where malicious nodes may collaborate to launch coordinated attacks.

Another solution suggested to deal with the problem of malicious node detection in WSNs is the implementation of a Secure Data Aggregation Protocol (SDAP). In order to improve accuracy and security against security threats, non-leaf nodes in this protocol's tree topology are subject to a high degree of trust, hence making it possible to identify rogue nodes. The efficiency and security of data collecting in WSNs are improved by this technology, which guarantees the safe aggregation of data. In conclusion, managing and detecting rogue nodes in wireless sensor networks (WSNs), particularly those that are a part of a cluster, is a challenging problem that calls for advanced methods and protocols. These include neighbor-based detection, secure data aggregation protocols, and cooperative bait detection approaches. By implementing these methods, WSNs can enhance their security and reliability, ensuring that the data collected is accurate and trustworthy.

Given the lack of direct information from the provided sources, I'll outline a general step-by-step process for detecting and predicting malicious data injection in Wireless Sensor Networks (WSNs) using improved swarm intelligence. The foundation of this procedure is the application of swarm intelligence principles to the particular issue of malicious data insertion.

Data Collection and Preprocessing

Sensor Data Collection: Initially, data is collected from various sensors within the WSN. This data can include environmental parameters, structural integrity measurements, etc.

Step1: Preprocessing: The collected data is preprocessed to remove noise and normalize the data. This step is crucial for ensuring that the data is in a suitable format for analysis.

Step2: Swarm Intelligence Algorithm Implementation

Swarm Initialization: A swarm of artificial agents (particles) is initialized. Each particle represents a potential solution to the problem of detecting malicious data injection.

Fitness Function Definition: A fitness function is defined to evaluate the quality of each particle's solution. In this context, a good solution would be one that accurately identifies malicious data injections.

Step 3: Swarm Behavior Implementation

Particle Movement: Each particle moves through the solution space, adjusting its position based on its own best solution and the best solutions of its neighbors. This movement is guided by the swarm intelligence algorithm, which can be inspired by natural phenomena such as bird flocking or fish schooling.

Collaboration and Competition: Particles collaborate by sharing their best solutions and compete by trying to find better solutions. This collaborative and competitive behavior helps the swarm to explore the solution space more effectively.

Step 4: Detection of Malicious Data Injection

Anomaly Detection: The swarm intelligence algorithm uses the collective intelligence of the swarm to identify anomalies in the sensor data. Anomalies could indicate malicious data injections.

Prediction of Future Attacks: By analyzing the patterns and behaviors of the swarm, the algorithm can predict future malicious data injections. This prediction capability allows the network to take proactive measures to mitigate the impact of such attacks.

Step 5: Action Based on Detection and Prediction

Isolation of Malicious Nodes: Once malicious data injections are detected, the algorithm can suggest isolating the compromised sensors to prevent further data corruption.

Preventive Measures: Based on the predictions of future attacks, the network can implement preventive measures, such as updating security protocols or deploying additional sensors to monitor for potential threats.

Step 6: Continuous Monitoring and Adaptation

Continuous Learning: The swarm intelligence algorithm continuously learns from the data collected and the actions taken. This learning process allows the algorithm to adapt to new types of malicious attacks and improve its detection and prediction capabilities over time.

Feedback Loop: The outcomes of the actions taken based on the algorithm's recommendations are fed back into the system. This feedback loop helps to refine the algorithm's strategies and improve its overall effectiveness.

This step-by-step process represents a high-level overview of how improved swarm intelligence can be used to detect and predict malicious data injection in WSNs. The specific implementation details, including the choice of swarm intelligence algorithm and the design of the fitness function, would depend on the specific requirements and constraints of the WSN.

II. RELATED WORKS

In the realm of wireless sensor networks (WSNs), ensuring data security is paramount, particularly when aggregating data from multiple sensors. This literature review delves into the intricate domain of secure data aggregation, focusing on the imperative task of filtering out the adverse impact of attackers. Scholars have extensively explored various techniques and protocols to fortify WSNs against malicious entities aiming to compromise data integrity and confidentiality during aggregation processes. From cryptographic mechanisms to anomaly detection algorithms, researchers have proposed multifaceted approaches to safeguard the aggregation process [1]. Additionally, studies have investigated the utilization of trust models and collaborative filtering techniques to discern trustworthy nodes from compromised ones, thus mitigating the attacker's influence on data aggregation. Furthermore, advancements in machine learning and artificial intelligence have been leveraged to enhance the detection and mitigation of attacks on WSNs, offering promising avenues for future research. This review synthesizes existing literature, highlighting both the challenges and advancements in the quest for secure data aggregation in wireless sensor networks, ultimately contributing to the establishment of robust and resilient network infrastructures in the face of evolving threats.

The study of fine particles thin films and exchange anisotropy has garnered significant attention in both scientific and technological realms due to its potential applications in various fields such as magnetic recording, spintronics, and magnetic sensors. Fine particles thin films, characterized by their nanoscale thickness and size, exhibit unique physical properties distinct from bulk materials, making them promising candidates for novel device architectures. Exchange anisotropy, a phenomenon arising from the coupling between ferromagnetic and antiferromagnetic materials at their interface, plays a crucial role in determining the magnetic behavior of thin films [2]. Understanding the intricate interplay between fine particles, thin film morphology, and exchange anisotropy is essential for optimizing material properties and enhancing device performance. This

literature review aims to provide a comprehensive overview of recent advancements, theoretical models, experimental techniques, and applications in this interdisciplinary field, shedding light on the underlying mechanisms governing the magnetic behavior of fine particles thin films and exchange anisotropy.

The design and implementation of clustering in Wireless Sensor Networks (WSNs) is a critical aspect impacting the network's performance, scalability, and energy efficiency. Clustering is a fundamental technique used to organize sensor nodes into groups, facilitating efficient data aggregation, routing, and management. Numerous studies have addressed various challenges and considerations in designing and implementing clustering algorithms in WSNs, such as the trade-off between energy consumption and network lifetime, the selection of cluster heads, communication overhead, and network topology dynamics [3]. Researchers have proposed diverse clustering approaches, including centralized, distributed, and hybrid schemes, each with its advantages and limitations. Additionally, issues like cluster formation, cluster head selection criteria, intra-cluster communication, data fusion, and cluster reorganization strategies have been extensively investigated to optimize network performance and prolong network lifetime. Despite significant progress, ongoing research efforts are necessary to address emerging issues such as node mobility, network heterogeneity, and security concerns, ensuring robust and efficient clustering solutions for future WSN deployments.

Security vulnerabilities in Wireless Sensor Networks (WSNs) have become a significant concern due to their widespread deployment in various applications. This survey aims to provide a comprehensive overview of the existing literature on security vulnerabilities in WSNs. The review encompasses a thorough analysis of different types of vulnerabilities such as physical attacks, node compromise, routing attacks, and cryptographic vulnerabilities, highlighting their potential impact on network integrity and data confidentiality [4]. Furthermore, this survey evaluates various security mechanisms and protocols proposed to mitigate these vulnerabilities, including encryption algorithms, authentication schemes, and intrusion detection systems. Through a systematic examination of research efforts in this domain, this literature review identifies emerging trends, challenges, and future directions for enhancing the security of WSNs, thereby contributing to the advancement of secure and reliable wireless sensing environments.

The efficient management of cryptographic keys in Wireless Sensor Networks (WSNs) is paramount for ensuring data confidentiality, integrity, and authenticity [5]. As these networks are deployed in diverse application scenarios with varying security requirements, selecting appropriate key management schemes becomes crucial. Numerous schemes have been proposed, each with its own strengths and weaknesses. Some prioritize energy efficiency, crucial for prolonging sensor network lifetime, while others emphasize scalability, adaptability to dynamic network topologies, or resistance against specific security threats. Commonly considered schemes include hierarchical, location-based, and probabilistic approaches, among others. Hierarchical schemes establish a layered key hierarchy to facilitate efficient key distribution and revocation, while location-based schemes leverage spatial proximity for key establishment. Probabilistic schemes, on the other hand, utilize random key predistribution to achieve resilience against node compromise. Evaluation criteria typically include computational overhead, communication overhead, resilience to node compromise, scalability, and energy efficiency. Choosing the most suitable key management scheme necessitates a thorough understanding of the application requirements and network characteristics, balanced against the inherent trade-offs in security, performance, and resource utilization.

III.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.

In order to find and eliminate dangerous network data, we have developed an algorithm. The suggested optimized swarm intelligence algorithm is applied to various datasets to assess its performance. A simulator is used to test the algorithm. The study's findings and simulations demonstrate how to recognize and fix erroneous data in wireless sensor networks.

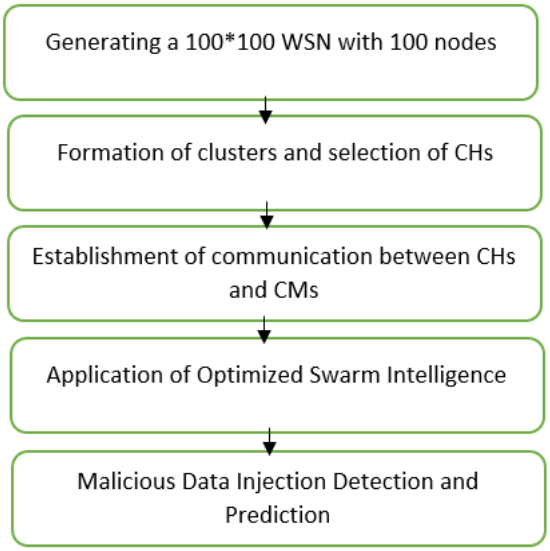

Fig 2: Block Diagram of Existing Method

In order to identify false alarms while detecting selfish nodes, the suggested technique computes the best path utilizing a hybrid combination of COA-EASRP and AODV in addition to TCM. Our suggested method offers the results of several simulations that were run depending on different parameters. We can expand on the knowledge and strategies discussed in the sources provided in order to carry on with the current approach of identifying and removing potentially harmful network data in wireless sensor networks (WSNs) utilizing an optimized swarm intelligence algorithm. By detecting and fixing faulty data, the aim is to improve the security and dependability of WSNs, which is important for applications like tracking events like fires and floods.

Enhance Anomaly Detection with Machine Learning: The integration of machine learning, specifically neural networks, with swarm intelligence algorithms can significantly improve the detection of anomalies in WSNs. The use of back propagation neural networks combined with evolutionary algorithms like Particle Swarm Optimization has shown promising results in optimizing the structure configuration of BPNN for identifying errors in WSNs.

Enhance Algorithms for Swarm Intelligence: PSO optimization, which entails the addition of a parallel mechanism for further tuning and a biological population model to control population size, can enhance the algorithm's performance. This improvement can decrease the false positive rate and increase accuracy, which will help WSNs detect faults more accurately.

Simulation and Experimental Validation: To validate the effectiveness of the enhanced swarm intelligence algorithm, simulation experiments should be conducted. The algorithm's performance should be assessed in these tests in terms of detection accuracy and false positive rate (FPR) across various datasets. The results from these simulations can provide insights into the algorithm's effectiveness in identifying and correcting dangerous network data.

Addressing Fault Types: Understanding and addressing different types of faults in WSNs, such as hardware faults, software faults, and persistent or transient faults, is crucial. The proposed algorithm should be capable of identifying these faults based on data characteristics, ensuring that both the detection accuracy and the false positive rate are optimized.

Future Research Directions: Continuing research should focus on further optimizing the population size

of evolutionary algorithms and introducing more mathematical theories and methods. Additionally, broadening the scope of applications and using computational intelligence to solve more practical problems can enhance the overall effectiveness of the algorithm in WSNs.

By building on these insights and techniques, the optimized swarm intelligence algorithm can be further refined to enhance the security and reliability of WSNs. By doing this, the network will be more resistant to both local and distant threats, safeguarding the accuracy of sensor readings that are vital to certain applications.
Cons: Because it refreshes the velocity, implementation is sluggish.
It employs a single implementation strategy-more consistent behavior.

IV. METHODOLOGY

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..

We have created an algorithm to identify and remove harmful network data. Using several datasets, the suggested optimal swarm intelligence method's performance is assessed. The simulator is used to test the method.The study's findings and simulations demonstrate how to recognize and fix faulty data in wireless sensor networks.

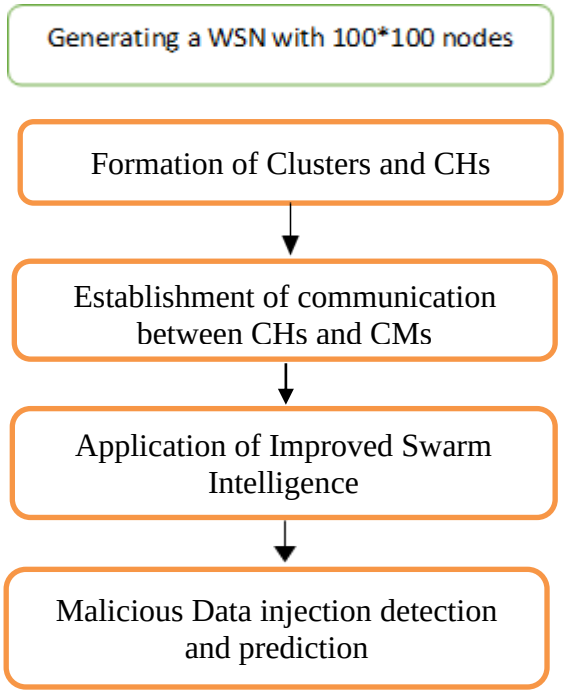

Fig. 3 : Proposed Method's Block Diagram

Proceeding from the suggested approach of utilizing an optimized swarm intelligence algorithm to identify and remove malicious network data in wireless sensor networks (WSNs), the subsequent actions can be implemented to augment WSN security and dependability even more:

Integration with Advanced Routing Algorithms: Building upon the Swarm-Intelligence-Centric Routing Algorithm (SICROA) for WSNs, integrating it with advanced routing algorithms like Ant Colony Optimization (ACO) can significantly improve the network's resilience against attacks. ACO is known for its ability to adapt to changes in the network environment and efficiently route data packets, which can be crucial for maintaining the integrity of sensor data in the face of physical or remote attacks.
Enhanced Collision Avoidance and Link Quality Prediction: Incorporating mechanisms for collision avoidance and link quality prediction within the SICROA can further enhance the network's security. By predicting link disconnections and maintaining the network's stability, the algorithm can prevent the

introduction of erroneous data due to failed transmissions or compromised links.

Energy Efficiency and Scalability: Ensuring that the algorithm is energy-efficient and scalable is essential for maintaining the operational lifespan of WSNs. This can be achieved by optimizing the routing process to minimize energy consumption while ensuring that the network can adapt to changes in the environment, such as the addition or removal of sensors.

Simulation and Experimental Validation: To validate the effectiveness of the enhanced algorithm, it is crucial to conduct simulation experiments. These experiments should evaluate the algorithm's performance in terms of security, reliability, and energy efficiency across various datasets and network conditions. The results from these simulations can provide insights into the algorithm's effectiveness in identifying and correcting harmful network data.

Adaptive Security Measures: Implementing adaptive security measures that can dynamically adjust to changes in the network environment is another important aspect. This could involve using machine learning techniques to continuously update the algorithm based on the latest data patterns and network conditions, thereby improving its ability to detect and eliminate harmful data.

Future Research Directions: Future research should focus on exploring the integration of other swarm intelligence techniques with the SICROA to further enhance its capabilities. Additionally, investigating the impact of different network conditions and attack scenarios on the algorithm's performance can provide valuable insights for future improvements 3.

By following these steps, To improve the security and dependability of WSNs, the suggested optimized swarm intelligence algorithm can be further improved. This would make the network more resistant to nearby and physical attacks and guarantee the integrity of sensor readings utilized in crucial applications.

Advantages:

- It don't updates the velocity which makes implementation faster.
- It uses two strategies for implementation which is less predictable behavior.

Applications:

- There are numerous applications for the use of real time applications, yet the following are the most typicalones: Networks of wireless sensors (WSN). Internet of Things systems (IoT).
- Attendance and Timing.Attacks on Security in Wireless Sensor Networks Various layers of wireless sensor networks are subject to various kinds of attacks. Malicious nodes and subversion are two possible attack types at the software layer.
- Techniques for identifying and isolating malicious nodes can help overcome this. The assaults that occur on the network layer are the sinkhole, wormhole, and Sybil attacks. Secure routing techniques and key management can be used to analyze this. DoS attacks are possible in the physical layer. Adaptive antennas and flexible spectrum are countermeasures that are meant to be seized. Physical Attacks: A physical attack could be used to force entry to the hardware. This raises a concern about Only be possible with additional steps, such as outdoor law enforcement. This increases the power of physical attacks as a substitute. They offer several possible advantages over far-reaching strikes. Records could be appropriately stored in encrypted format on portable computer systems as well, but usability and accessibility issues frequently prevent this from happening. Because of this, gaining physical access to a laptop device typically grants full access to the stored data, along with the ability to perform changes. It can be obtained at an indeterminate point in the future during an attack, which isn't always feasible during protracted attacks. Physical

evidence aims to manually attribute statistics that are indecently assigned to a person or organization.

Such forwarding phony routing facts, selective forwarding, sink hollow wormholes, hey floods. clump based totally protocols (LEACH, teenager, PEGASIS) selective forwarding selective forwarding sink hole, wormholes, Sybil power holding topology protection (SPAN,GAF,CEC, International Journal of Pure and Applied Mathematics Special Issue 396 AFECA) phony routing statistics, Sybil, hey floods. Safety protocols are secure network enabling Protocol (SNEP) that provides confidentiality, authentication and small regular inexperienced movement Loss (μ TESLA) offers documented broadcast. Comfortable network coding Protocol (SNEP). 3. Comparison Study of Malicious Node Detection based on Optimization Methods In this comparison study we are dealing with two optimization methods they are:-

1. CREATED HONEYBEE
2. CUCKOO SEARCH

Artificial Honeybee

The artificial bee colony (ABC) set of recommendations is a modern swarm intelligence set of rules that are modeled after the behavior of honey bees.

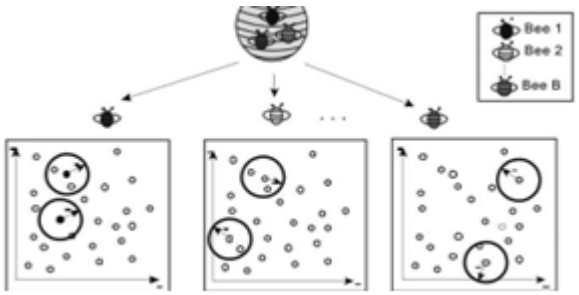

Fig 4: Artificial Bee Colony Optimization

The Artificial Bee Colony method is one such optimization technique. It is a cross between particle swarm optimization and genetic algorithms. This software emulates the foraging habits of honey bees. The artificial bee colony consists of three distinct types of bees: scout, observer, and employed bees. In general, both the food and the observer bees are similar in size. Every worker bee has a single feeding source. The bee's dance helps the onlooker bee select the food source. The scout bees find new food sources to replenish the ones they left behind. The ABC algorithm determines the best option for determining the path to take in order to reach the goal based on this idea.

Dynamic Clustering based Approach

A dynamic clustering-based technique called DCAD was proposed by Alikhany et al. for anomaly identification in AODV-based fully MANETs. It employs a set of weighted regular width clustering algorithms to identify routing attacks and provide a profile of typical community behavior. Furthermore, it updates the profile on a periodic basis using a forgetting equation. The results of the experiment validate that DCAD has an excessive false alarm charge.

Cuckoo's Search Optimization

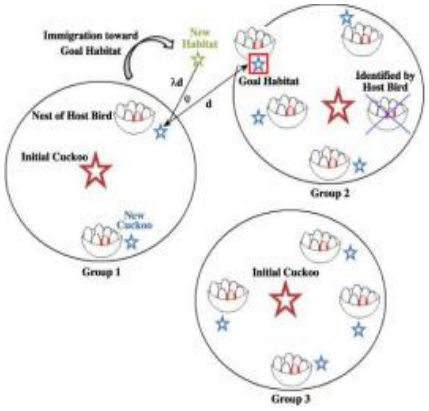

Fig 5: Cuckoo Search

In the current work, consider and energy aware Routing Protocol (TERP) is introduced for achieving the secured and electricity concerned packet transit. The various deployment usage of wireless sensor networks leads to a multiplicity of issues, including safety threat, lacks of resource availability International Journal of Pure and Applied Mathematics Special Issue 399, and so forth. These

issues need to be resolved to be able to advantage an advanced consciousness of researchers and customers to deploy the features of WSN regularly. The most crucial assignment inside the WSN is records transmission, which can't be done securely and reliably due to an inappropriate route life. As a result, the focus at the better course discovery can clear up these issues in the optimized way.

Cuckoo seek is a set of principles employed for accepted as true and reliability-conscious course status quo in proposed research paintings. Following the current state of the course, Trojan horse attacks are detected using the estimated cost of packet transmission.

V. RESULTS AND DISCUSSIONS

Following the identification and removal of malicious nodes from the route, the path to BS was created and represented in the image below.

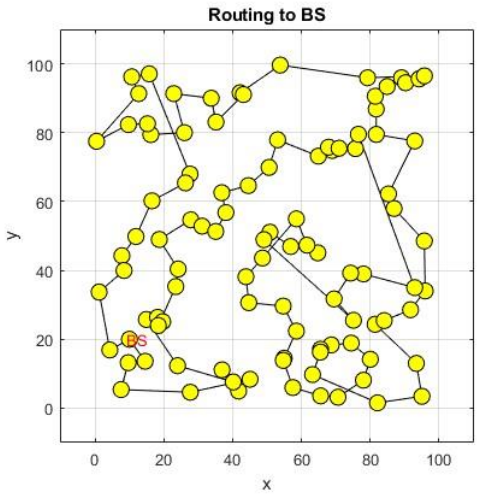

Fig 6: Routing Through IPSO

The picture below illustrates how the number of malicious nodes discovered by the proposed IPSO algorithms and the current OPSO algorithms compare. It is clear from this comparison that the IPSO recognition rate improved more steadily than the OPSO.

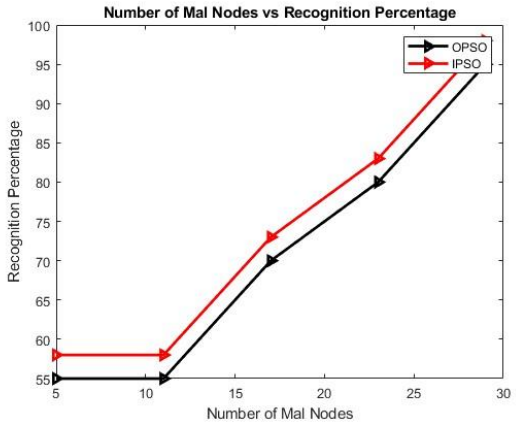

Fig 7: Number of Mal Nodes Vs Recognition Percentage

The picture below illustrates how the number of normal nodes detected by the proposed IPSO algorithms and the current OPSO algorithms compare. It is clear that the IPSO algorithms attained the desired level more quickly and with a substantially lower false positive rate than the OPSO techniques.

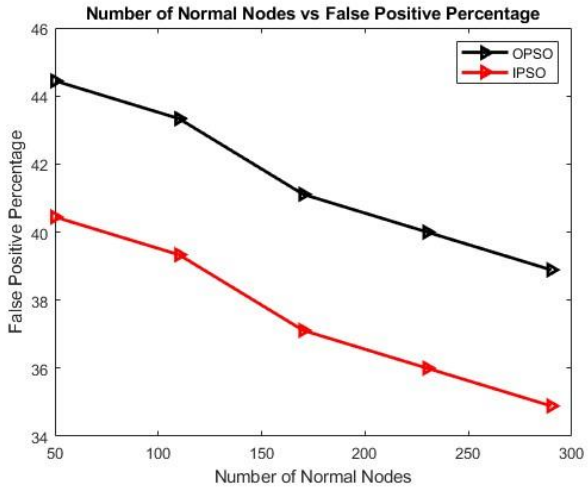

Fig 8: Number of Normal Nodes Vs False Positive Percentage

The OPSO method was used to identify malicious nodes, which were then plotted in the picture below. It is evident that the rate of malicious nodes is larger than the proportion of malicious nodes that was initially taken.

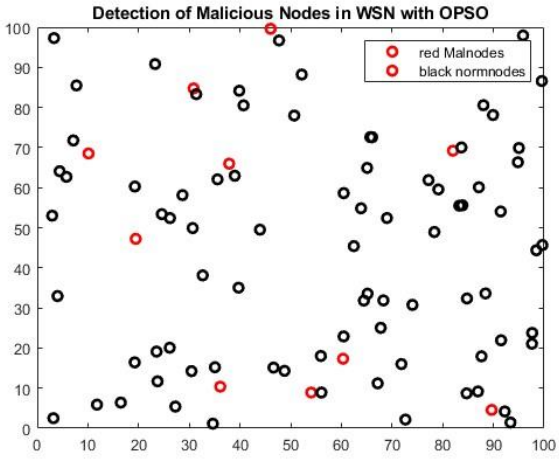

Fig 9: OPSO Detected Malicious Nodes

The detected malicious nodes using IPSO algorithm was plotted in the below figure. It can be shown that the malicious nodes are at a nearly similar rate compared with the initially taken malicious node percentage value.

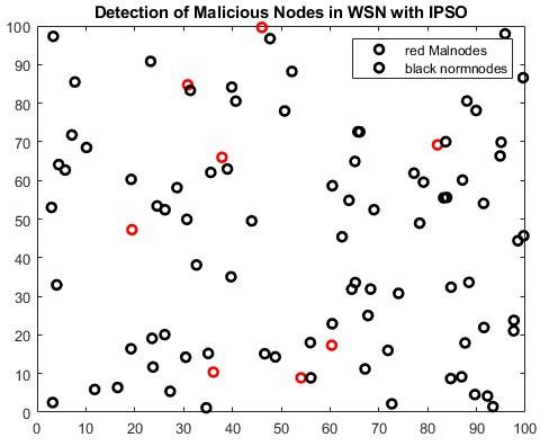

Fig 10: IPSO Detected Malicious Nodes

VI. CONCLUSION

The investigation on malicious data injection detection and prediction in wireless sensor networks (WSNs) using enhanced swarm intelligence can be concluded using the insights and findings offered in the sources supplied. Through research and simulations conducted on a variety of datasets, the optimized swarm intelligence algorithm has demonstrated its effectiveness in identifying and mitigating the risks associated with malicious data injection attacks in wireless sensor networks (WSNs). In conclusion, the use of improved swarm intelligence algorithms for detecting and predicting malicious data injection in WSNs has resulted in a significant advancement in WSN security. These algorithms not only facilitate threat identification and mitigation, but they also create new research and development opportunities for WSN security.

VII. REFERENCES

[1]. Roy Sandip et al., "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681-694, 2014.

[2]. I. S. Jacobs, C. P. Bean, G. T. Rado, H. Suhl, "Fine particles thin films and exchange anisotropy" in Magnetism, New York:Academic, vol. III, pp. 271-350, 1963.

[3]. K.Pradeepa, WR Anne, S.Duraisamy, "Design and implementation issues of clustering in Wireless Sensor Networks", International Journal of Computer Applications, vol. 47, no. 11, pp. 23, 2012.

[4]. T Kavitha, D.Sridharan, "Security vulnerabilities in Wireless Sensor Networks: A survey", Journal of Information Assurance and Security, vol. 5, pp. 31-44, 2010.

[5]. C.Alcaraz, J Lopez, R Roman, "Selecting Key Management Schemes for Wireless Sensor Networks application", Journal of Computers and Security (Elsevier), vol. 31, no. 8, pp. 956-966, 2012.

[6]. R Azarderskhsh, A Reyhani, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks", Eurasip Journal on Wireless Communications and Networking Article ID: 893592, pp. 1-12, 2011.

[7]. AC Chan, C Castelluccia, "A security framework for privacy preserving data aggregation in wireless sensor networks", ACM Transactions on Sensor Networks (TOSN), vol. 7, no. 4, pp. 29, 2011.

[8]. S.Chatterjea, P. Havinga, "A Dynamic data aggregation scheme for Wireless Sensor Networks", Proc. ProRISC, pp. 56-60, 2003.

[9]. Dietrich, F. Dressler, "On the Lifetime of Wireless Sensor Networks", ACM Transactions on Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009, [online] Available: 10.1145/1464420.1464425. [10] K. Kalpakis, K. Dasgupta, P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks", Computer Networks, vol. 42, no. 6, pp. 697-716, August 2003.

[10]. Y. Xue, Y. Cui, K. Nahrstedt, "Maximizing lifetime for data aggregation in wireless sensor networks", ACM/Kluwer Mobile Networks and Applications (MONET) Special Issue on Energy Constraints and Lifetime Performance in Wireless Sensor Networks, pp. 853-64, Dec. 2005.

[11]. B. Hong, V.K. Prasanna, "Optimizing system lifetime for data gathering in networked sensor systems", Workshop on Algorithms for Wireless and Ad-hoc Networks (A-SWAN), August 2004.

[12]. K. Kalpakis, K. Dasgupta, P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks", Computer Networks, vol. 42, no. 6, pp. 697- 716, August 2003.

[13]. S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management," 2021 IEEE Symposium on Computers and Communications, Marrakech, 2021, pp. 537-542.

[14]. C. Blum, and X. Li, “Swarm intelligence in optimization,” Swarm Intelligence . Springer, Berlin, Heidelberg. pp. 43-85, 2018.

[15]. D. Karaboga, “An idea based on honey bee swarm for numerical Optimization,” Erciyes university, engineering faculty, computer engineering department. 2015.

[16]. J. Singh, R. kumar and A. K. Mishra, "Clustering algorithms for wireless sensor networks: A review," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 637- 642.

[17]. F. Ishmanov, and Y. Bin Zikria, “Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues,” Journal of Sensors, 2020.

[18]. Benjie Chen, Kyle Jamieson, Hari Balakrishnan And Robert Morris “An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks,” in Proceedings of the wireless network, 2019.