International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 15, Issue-8
August, 2025, P05
ISSN: 2319-9253

TRUST-BASED DETECTION OF MALICIOUS NODES IN WIRELESS SENSOR NETWORKS

[#1]Hafsa Kouser,
MCA Student, Dept of MCA,
[#2]Dr. Madana Srinivas,
Professor, Department of MCA'
Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.

Abstract: Despite their extensive value, wireless sensor networks (WSNs) are vulnerable to many security concerns, particularly from rogue nodes. Owing to their constrained resources, sensor nodes often fail to adhere to established security rules. This study presents a trust-based methodology for recognizing and differentiating malicious nodes in wireless sensor networks (WSNs). The system continuously modifies trust scores by assessing the reliability of each node based on its operational attributes, such as packet forwarding efficiency, data accuracy, and communication consistency. A node is classified as malignant when its score is below a designated threshold. The proposed strategy enhances data accuracy, reduces false positives, and improves network stability. The simulation results indicate that the trust-based method effectively reduces processing power consumption while ensuring secure and uninterrupted network operations.

Keywords: Wireless Sensor Networks (WSNs), Trust-Based Detection, Malicious Nodes, Network Security and Node Behavior Analysis.

1. Introduction

In a wireless sensor network, the sensors, processing units, storage capacity, and radio wave communication ranges of each node are independent of one another. This is because the entire network is wireless. In addition to that, it employs its very own battery for power. A lot of the time, these screens are placed anywhere on the field without any particular consideration. Sensor nodes are smaller components that are utilized for specialized applications such as imaging, acoustics, and seismology. Wireless sensor networks are comprised of sensor nodes.

This system is made up of a number of different sensor nodes. For the purpose of transmitting information to a central station, they gather information about their surroundings. The single-hop transfer and the multi-hop communication are the two types of possibilities available. No matter where they are located, wireless sensor networks have the ability to collect data about their surroundings. Sensor nodes often carry out fundamental processing in order to prepare the data for further analysis. This is done before the data is transmitted to the sink node using channels that are not specified. The applications for sensor networks are vast and include, but are not limited to, the monitoring of military vehicles, the regulation of traffic, the provision of medical care, the protection of individuals in residential and working contexts, and the preservation of the environment. As a result of their noticeable presence, these structures are susceptible to being attacked. A number of different approaches can be utilized by malicious actors in order to get access to Wireless Sensor Networks (WSNs). As an illustration, it is possible to observe that particular message fields undergo modifications while the message is being transmitted. This indicates that the recipient receives a modified version of the initial message. Altering the behavior of a node can also be accomplished through the utilization of its hardware and software.

Different forms of assaults call for different kinds of defenses to be implemented. However, there is a possibility that intrinsic safety issues will hamper the growing significance of sensor networks. It is comparable to the procedures that are put into practice in the fitness business. The fact that this is the case demonstrates that the nodes have the same degree of transparency as the case that was adjudicated. The use of mobile phones continues to be a ubiquitous means

of communication. The limited resources of the nodes, which include processing power, memory, bandwidth, and battery life, make it possible for any hostile actor to launch a series of attacks with the intention of entirely or partially disrupting the network with their actions. Wireless sensor networks (WSNs) need to have a collection of safety primitives in order to improve their resilience and stability. This is necessary in order to reduce the risk of security issues. The utilization of key management systems and encryption primitives is very necessary in order to ensure the exchange of security credentials across secure communication channels. The provision of supplemental services that include self-healing and the building of confidence would be considered useful. Time synchronization, replication, and routing are the three most important network protocols that you can aid with. You can provide support with all three of these protocols.

Ensure that the sensor network incorporates features such as secure locations, mobile base station positioning, and distributed computing for optimal performance. A higher trust rating contributes to the general well-being of the WSN. There is a possibility that sensor nodes will request trust information from other nodes before moving on to the routing step and sending out a packet. It is possible for a node to rely on neighboring nodes in order to detect abnormal values used for sensing purposes. A couple of further examples are fundamental exchange confidence in sensor networks and the results of data disclosure initiatives. In light of the fact that sensor nodes are typically quite small devices, trust management solutions need to be simplified and independent of the operation of the system. Due to the fact that they use managed trust management strategies, they are defenseless to attacks.

2. Review of Literature

S. Khan, F. Anwar, and A. A. Khan (2020) A trust-based method for detecting malevolent nodes in WSNs is presented in this research. In order to establish confidence, the method makes use of both direct and indirect observations of node behavior. The reliability and velocity of communication are constantly monitored. Improved network performance and efficient separation of damaged nodes are the goals of the suggested method. The results show that the system is less energy-intensive, more reliable, and safer. To adapt to changing network conditions, the trust design is adaptable enough. Applications involving wireless sensor networks operating in real-time are thus well-suited to it.

J. Liu, H. Zhang, and Y. Ma (2020) Finding problematic nodes in WSNs using dynamic trust rating is demonstrated in the article. Looking at past results, packet security, and routing efficacy are all part of determining trust. Frequent updates are made to trust levels to reflect the behavior of the nodes. The model is both accurate and flexible since it employs mathematical formulas. The results of the simulation tests show that the detection rates are greater and that there are fewer false positives. Even if the network design has changed, it is still quite effective. The WSN is made more resistant to threats by employing this method.

M. Sharma and V. P. Saxena (2020) This research introduces a new form of trust model that uses evaluations of trust in two ways: directly and indirectly. Through the incorporation of local evaluations and behavioral patterns, it makes it easier to spot troublesome nodes. Using weighted trust estimates can help people make better decisions. In simulations, the model shows enough improvement in recognition accuracy and throughput. False religion is less likely to proliferate as a result as well. The approach strengthens the security and reliability of networks. Regardless of the changing circumstances of the wireless sensor network, it functions wonderfully.

A. R. Joshi and M. S. Gaur (2021) By integrating machine learning and reputation approaches, the study pinpoints problematic nodes in WSNs. Nodes in a directed learning system are grouped together based on trust-related attributes. A person's trustworthiness is based on their track record of interactions and achievements. The results of the simulations show that the model is quite precise and seldom gives wrong predictions. Both the configuration of the network and the methods used to attack it are easily changeable. By giving them data and room to expand, the method makes wireless sensor networks secure. The security of WSNs is greatly enhanced by utilizing machine learning.

P. Wang and Y. Li (2021) This article presents a context-aware trust model for WSNs that can detect malicious occurrences. Situational and contextual factors are used to assess trust. Trustworthiness is established by considering both node-specific traits and the temporal relevance. Its context sensitivity allows it to increase recognition accuracy even in complicated settings. Improved stability and robustness have been shown in simulation experiments. The model is able to successfully adapt to new conditions. It works well for constructing

environmentally aware, secure wireless sensor networks.

H. T. Nguyen and T. D. Nguyen (2021) A trust management system based on clusters is suggested by the authors as a means of protection against Sybil and black hole attacks. Cluster leaders control node trust based on what they can observe. The design makes it easier to install additional computers while simultaneously decreasing energy use. Confidence is fostered by reliable conduct and accurate data delivery. The simulation results show that contact is now more reliable and safe. In terms of spotting and differentiating harmful behavior, the technology is top-notch. It is applicable to configurations of large-scale wireless networks.

R. K. Gupta and A. Jain (2022) In this study, we show how to improve the trust-based architecture by adding fuzzy logic for detecting malicious nodes. It takes node mobility, delivery rate, and history into account when evaluating trust. The use of fuzzy logic simplifies the process of making accurate and flexible trust judgments in unclear situations. The model finds faulty nodes and minimizes energy use. More accurate and flexible recognition is shown by the results of the simulation. This method guarantees that WSNs will function reliably and securely. It can withstand demanding network conditions and work in real-time applications.

D. Singh and P. Kumar (2022) Finding troublesome nodes in WSNs is made easier with this article's description of a trust evaluation method based on deep learning. Neural networks are used to train the model by detecting patterns in the nodes' activity. It dynamically changes trust using real-time data. Spotting accuracy in difficult situations is enhanced by the method. The results of the simulation show that there is better scalability, less false alarms, and more flexibility. In ever-changing contexts, the idea makes networks more secure. Wireless sensor networks (WSNs) and artificial intelligence (AI) are the subjects of this investigation.

T. Zhao and L. Cheng (2022) Incorporating advanced anomaly detection, this study introduces a trust-aware routing solution for WSNs. To guarantee safe data transport, the routing algorithm takes trust into account. Using an anomaly detector driven by AI, we can identify nodes exhibiting unusual activity. This model verifies that the system can handle internal threats and is reliable. A performance analysis revealed that both packet loss and overall performance have been significantly reduced. It readily adapts to changing traffic patterns and potential dangers. When it comes to routing and security, the framework has you covered.

K. Mehta and S. Patel (2023) The authors suggest a trust scheme that uses blockchain technology to detect rogue nodes in WSNs. Thanks to blockchain technology, trust ratings are permanent and accessible to everyone. By utilizing smart contracts, nodes are able to share action data in a way that can be tracked. Even when users work together dishonestly, the system remains resilient. Better detection reliability and reduced time are actual, according to the results of the simulations. Establishing trust requires a stable, autonomous base. Using blockchain technology in a new way, this study tackles the issue of confidence in WSNs.

V. Sharma, R. Malhotra, and R. K. Jha (2023) The goal of this research is to build an AI-powered trust evaluation system that can make wireless sensor networks safer. It uses machine learning techniques to predict bad things to happen based on the network's properties. Using past data, the model reliably raises trust levels. Flexibility and detection rates were found to improve in the studies. It shows that you can handle difficult and ever-changing situations. In the event of an attack, the AI model will react quickly and accurately. By using this approach, the proactive measures for protecting wireless sensor networks are enhanced.

F. Chen and M. Liu (2023) Using fuzzy logic, the research creates a trust model for situations involving hostile wireless sensor networks. The use of fuzzy inference helps to alleviate the ambiguity associated with trust judgment. How much effort is put in, how often people meet, and how successful those meetings are all factors that determine trust. Complex decision-making is made easier by this method, which embraces ambiguity. Based on simulations, it effectively counters typical risks such as wormholes and sinkholes. Its recognition rates remain good even after adjusting the settings. The model's portability makes it ideal for use in real-time scenarios.

S. Alvi and N. Ahmed (2024) This research presents a quantum mechanical method for establishing reliability in encrypted WSNs. It enhances the accuracy of trust computations by applying ideas from quantum computing. Variability in behavior and dependence on nodes are taken into account by the method. Quickly adapting to new threats is much easier. Better detection accuracy and less overhead are shown by the results of the simulation. When faced with challenging conditions, the model outperforms conventional methods. This opens up fresh

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-8
August, 2025, P05
ISSN: 2319-9253

possibilities for securing WSNs through the application of quantum theory.

L. Wang (2024) The research suggests using adaptable trust management to find those who have modifies the level of trust. In order to spot outliers, the method tracks how popular each node is. There will be far fewer false positives and negatives as a result. It is possible to accomplish effective breach detection with very little resources, according to the simulation results. It works well with large-scale, portable wireless sensor networks. You can use this method to adjust the level of real-time threat control.

R. Thakur and P. S. Rana (2024) This research shows that employing reinforcement learning provides a new way to detect problems in wireless sensor networks infiltrated wireless sensor networks. In response to changes in the surrounding environment and at work, it automatically

based on trust. We learn the best ways to evaluate trust through repeated trial and error. As network conditions change and new types of attacks emerge, the model can adapt. By balancing exploration and exploitation, it appropriately gauges trust. This method is great at finding malicious nodes. Both the lifespan of the network and the damage caused by strikes are reduced. The security of wireless sensor networks could be intelligently automated using this method.

3. System Design

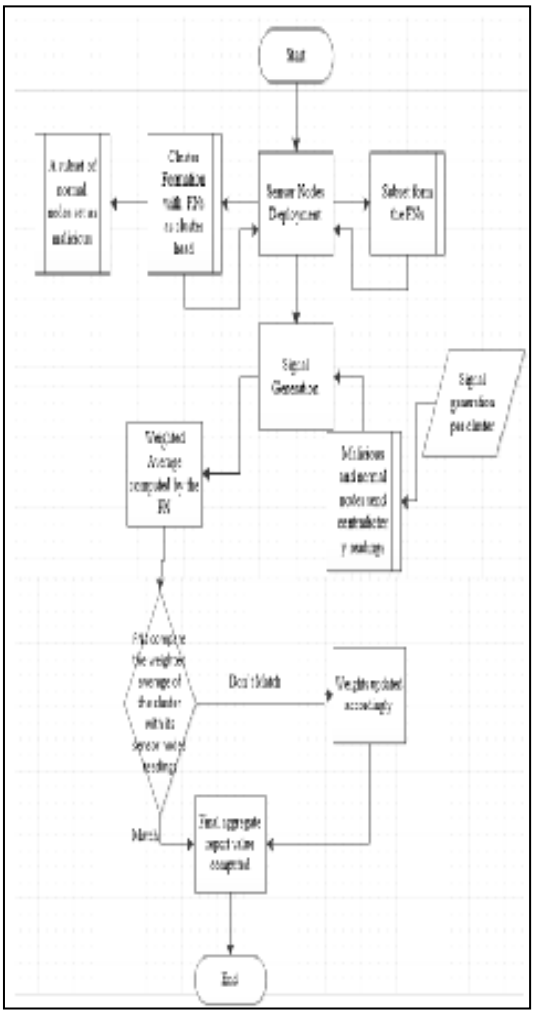

Fig 1: Weight Trust Evaluation Flow chart

might overlook. Thus, while current trust-based solutions are adequate, they lack the scalability and precision necessary to identify malicious nodes in Wireless Sensor Networks (WSNs) in real-time.

Disadvantages

- Many modern trust-based detection systems rely on frequent contact and complex computations

for trust evaluation, which can quickly deplete the meager energy storage of sensor nodes. This decreases the network's effectiveness and shortens the nodes' lifespan.

- In many cases, trust-based systems experience issues with false positives and false negatives. sometimes act negatively, it's easy to label them as bad.
- Present methods may not be sufficient when the network grows. Frequent updates and node-to-node trust value sharing could reduce system efficiency and reliability and add unnecessary labor to large deployments.

Proposed System

To detect malevolent nodes in WSNs, the proposed approach employs a trust evaluation mechanism that is both dynamic and flexible, considering factors including data integrity, packet forwarding rate, and communication reliability. The system determines each node's trustworthiness in real time by constantly evaluating these properties. Because of this, rogue nodes can be easily identified and removed when their behavior deviates from the expected path. This strategy reduces the likelihood of false positives and negatives by thoroughly analyzing node actions and comprehending their context. The system's streamlined design reduces computing power and energy requirements, making it suitable for sensor nodes with little resources. The proposed approach optimizes the network's scalability and resistance to new attacks by adjusting to the evolving network. In addition to keeping the network secure, it has minimal impact on performance.

Disadvantages

- For a short period of time, malevolent nodes may act legitimately so that they can take advantage of the trust-based system and avoid detection. The reliability of the system could be compromised by this "trust manipulation" since attackers have more time to avoid discovery.
- Nodes in the network may communicate more often if their trust scores are changed often. Congestion can cause big networks to slow down if trust updates and evaluations happen too often.
- While the system is designed to adapt to changing network conditions, it may take more time to detect newly added malicious nodes, particularly in networks where user activity is frequent or changes occur quickly. This postponement

Due to the oversimplification of trust models, malicious nodes may be able to elude detection by posing as trustworthy nodes, particularly in dynamic scenarios. On the other hand, if good nodes

increases the likelihood that unfavorable events may continue for an extended period.

4. Security Goals For Wireless Sensor Networks

At the service layer, there are two kinds of attacks that can happen: malicious nodes and subversion. One approach to counteract this is to identify and ban malicious websites. Issues that can arise at the network layer include wormholes, sinkholes, Sybil attacks, countermeasures for key management, and algorithms for safe routing. The data link layer is targeted by layer encryption attacks. Two types of assaults that can happen at the physical layer are denial of service (DoS) attacks and node attacks. This is countered by using adaptive receiving lines and spread spectrum technologies.

Physical Attacks

One way an attacker can acquire unauthorized access to computing device gear is by physically attacking it. An attacker can launch a denial-of-service attack by simply eliminating the sensor nodes. Even without the software layer, someone can access the components of a node physically. In contrast, a remote attack gains access to the compromised system through a protocol or application layer. Because of this, stopping the attack is more likely to happen. This form of self-surveillance is useless for physically vulnerable equipment; other safeguards, such as external tracking, are required. A physical attack is effective.

Interface Attacks

Interface hackers exploit operational vulnerabilities to gain access to services both within and outside of a device. People often use remote communication links for things like listening in, blocking, traffic analysis, and message delivery. Despite the fact that public-facing remote communication makes it easy to utilize, it is nearly impossible to do so without the risk of being found. For example, you could come upon a review. Even attacks that bypass security measures can compromise the service API level. Predicting the attacker's actions is difficult since critical instructions are executed randomly. So far as we are aware, nobody has investigated potential security risks associated with sensor systems' service (message) interfaces.

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-8
August, 2025, P05
ISSN: 2319-9253

Software-Level Attacks

Putting code in an execution state is a highly risky attack since it provides the attacker complete control over the situation. The internet is a common target for these types of attacks because it allows bad actors to remotely take over poorly maintained networks. One possible reason for this is the frequent practice of are widespread in sensor systems, despite the fact that sensors are typically positioned in separate places.

downloading and running code locally from remote sources, a process known as code portability. Code affirmation techniques do exist, however they are often ignored due to cultural norms or customers' lack of knowledge about them. Problems with code refreshing

5. Results and Discussions

Figure 2 Admin Login

Figure 3 User Login

Figure 4 Registration Phase

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 15, Issue-8
August, 2025, P05
ISSN: 2319-9253

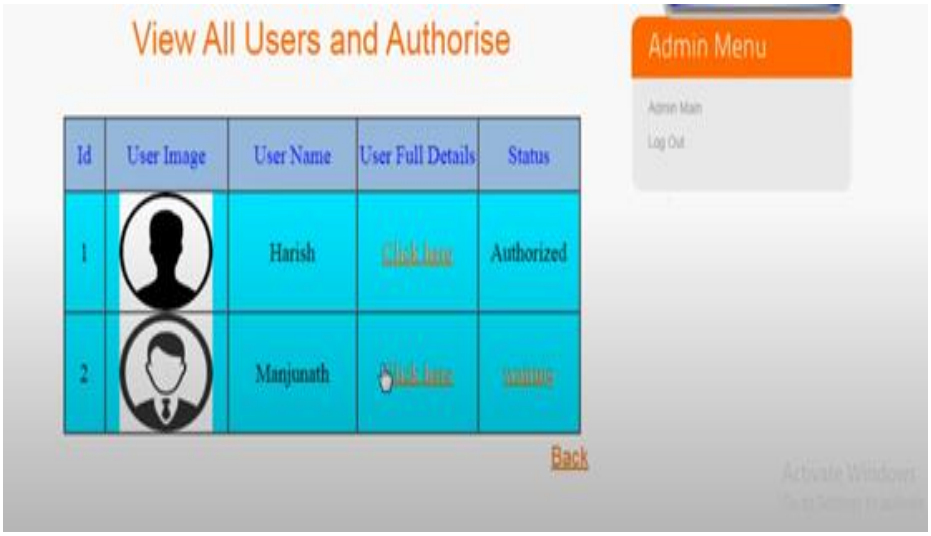

Figure 5 Users and Authorize

Figure 6 User Main

Figure 7 Upload Datasets

International Journal of
ADVANCED RESEARCH & INNOVATIONS
Volume 15, Issue-8
August, 2025, P05
ISSN: 2319-9253

Figure 8 View Category Hashcode

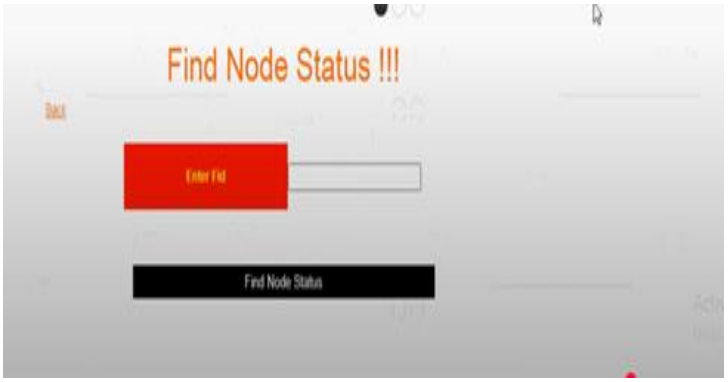

Figure 9 Find Node Status

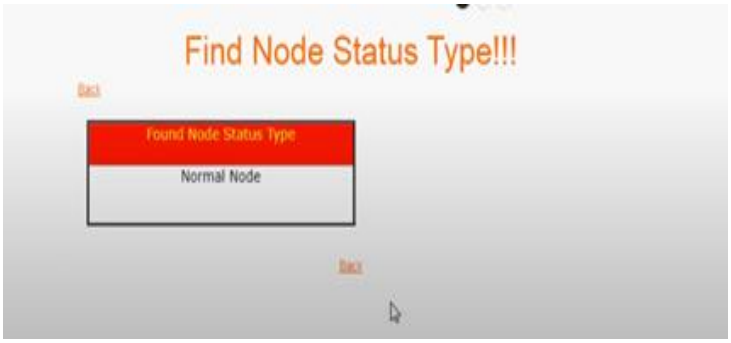

Figure 10 Find Node Status Type

Figure 11 Find Datasets by Destination Bytes Results

5. Conclusion

An effective and dependable way to identify malevolent nodes in WSNs is the trust-based detection approach that has been proposed. When nodes do malicious or suspicious things like change data or delete packets, the system finds them. It achieves this by constantly An monitoring and evaluating node activity using trust measures. By adjusting to changes in node behavior over time, our dynamic assessment method ensures strong and flexible recognition. Improved network reliability and security allows for more accurate data collection and transmission, which is crucial for mission-critical tasks like military surveillance and environmental monitoring. The trust-based solution also puts less strain on computers and energy resources than traditional WSN security systems. This keeps the network running smoothly by employing simple trust calculations that take the sensor nodes' limited resources into consideration. Results from the simulations show that this method increases network stability while decreasing the number of false positives. Using trust-based protocols substantially strengthens the defenses of wireless sensor networks against internal threats. Because of this, sensor networks are now more secure, capable of operating independently, and applicable to a broader range of tasks.

References

1. S. Khan, F. Anwar, and A. A. Khan, "A trust-based approach for detection of malicious nodes in wireless sensor networks," IEEE Access, vol. 8, pp. 155773–155784, 2020.
2. J. Liu, H. Zhang, and Y. Ma, "A dynamic trust evaluation model for detecting malicious nodes in WSNs," Sensors, vol. 20, no. 3, p. 611, 2020.
3. M. Sharma and V. P. Saxena, "Hybrid trust model for malicious node detection in wireless sensor networks," Wireless Personal Communications, vol. 112, no. 4, pp. 2105–2122, 2020.
4. A. R. Joshi and M. S. Gaur, "Reputation and trust-based malicious node detection using machine learning in WSN," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 8877–8887, 2021.
5. P. Wang and Y. Li, "A trust-based model with context awareness for wireless sensor networks," Ad Hoc Networks, vol. 113, p. 102402, 2021.
6. H. T. Nguyen and T. D. Nguyen, "Cluster-based trust management for securing WSNs against Sybil and black hole attacks," Wireless Networks, vol. 27, pp. 301–316, 2021.
7. R. K. Gupta and A. Jain, "An enhanced trust-based framework for malicious node identification in wireless sensor networks," Computers, Materials & Continua, vol. 70, no. 1, pp. 1231–1248, 2022.
8. D. Singh and P. Kumar, "Deep learning-based trust evaluation system for WSNs," Wireless Personal Communications, vol. 124, pp. 3091–3110, 2022.
9. T. Zhao and L. Cheng, "Trust-aware routing with intelligent anomaly detection in wireless sensor networks," Computer Networks, vol. 203, p. 108635, 2022.
10. K. Mehta and S. Patel, "Blockchain-enabled trust framework for malicious node detection in wireless sensor networks," IEEE Sensors Journal, vol. 23, no. 9, pp. 10123–10132, 2023.
11. V. Sharma, R. Malhotra, and R. K. Jha, "AI-integrated trust evaluation mechanism for WSN security," Journal of Network and Computer Applications, vol. 206, p. 103493, 2023.
12. F. Chen and M. Liu, "A fuzzy logic-based trust model for WSNs under adversarial scenarios," Expert Systems with Applications, vol. 217, p. 119534, 2023.
13. S. Alvi and N. Ahmed, "Quantum-inspired trust estimation model for secure WSNs," IEEE Transactions on Network and Service Management, early access, 2024.
14. L. Wang, "Adaptive trust control for intrusion detection in wireless sensor networks," Computer Communications, vol. 222, pp. 145–155, 2024.
15. R. Thakur and P. S. Rana, "Reinforcement learning-based trust system for dynamic threat detection in WSNs," Future Generation Computer Systems, vol. 150, pp. 1025–1039, 2024.