International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 10, Issue 6, June-2025, http://ijmec.com/, ISSN: 2456-4265

Reputation mechanism based secured CSS strategy on CWS network

R. Vyshnavi, Kathula Ashalatha, Asma Begum, Kuppireddy Dharani

[1]Assistant Professor,ECE Department Bhoj Reddy Engineering College for Women

[2,3,4]B. Tech Students, Department Of Ece, Bhoj Reddy Engineering College For Women, India.

ABSTRACT

Cooperative spectrum sensing can be regarded as a promising method to resolve the spectrum scarcity owing to achieving spatial diversity gain in cognitive radio sensor networks. However, the spectrum sensing data falsification attack launched by the malicious nodes will result in the wrong decision in the fusion center owing to the falsified observations. It will cause a serious security threat and degrade the decision making process. In this Project—, we propose a secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks to counter above kind of attack. The beta reputation model is applied to assign reputation value to cognitive sensor nodes according to their historical sensing behavior, and a dynamic trust evaluation scheme of cooperative spectrum sensing is established. In the final decision, the fusion center allocates a reasonable weight value according to the evaluation of the submitted observations to improve the accuracy of the sensing results. Simulation results support that our proposed strategy can weaken the impact of sensing data falsification attacks in cooperative sensing and outperform some traditional methods.

1- INTRODUCTION

Cognitive Wireless Sensor Networks (CWSNs) are an innovative extension of wireless sensor networks (WSNs) that leverage cognitive radio capabilities to efficiently utilize the available spectrum. In such networks, cooperative spectrum sensing (CSS) plays a vital role in ensuring reliable spectrum availability by allowing sensor nodes to collaborate in detecting spectrum holes. However, this cooperation is vulnerable to security threats, such as malicious attacks and misreporting by compromised nodes, which can degrade the overall performance of the network.

To address these challenges, a reputation-based secured cooperative spectrum sensing strategy is proposed. This approach integrates a reputation mechanism to evaluate and monitor the trustworthiness of individual sensor nodes based on their sensing behavior over time. By identifying and isolating malicious or unreliable nodes, the system enhances the reliability and accuracy of spectrum sensing. The mechanism further incorporates lightweight security techniques to ensure minimal resource consumption, which is crucial in resource-constrained CWSNs.

This project aims to design, implement, and evaluate a secured reputation-based CSS strategy to mitigate malicious threats, improve sensing accuracy, and maintain the integrity of the CWSN. The proposed solution will be tested under various network scenarios and threat models to validate its effectiveness, scalability, and adaptability in real-world conditions.

2-LITERATURE SURVEY

The development of Cognitive Wireless Sensor Networks (CWSNs) has garnered significant attention due to their ability to address the growing

problem of spectrum scarcity. In CWSNs, efficient spectrum sensing is essential to enable cognitive radios to detect available spectrum and make intelligent decisions regarding spectrum access. As the networks rely on spectrum sensing to avoid interference with primary users and utilize underused frequency bands, various sensing techniques have been explored and applied. However, with the increasing complexity and adversarial nature of these networks, security challenges, particularly attacks on spectrum sensing, have emerged as a critical concern. This literature review presents an overview of spectrum sensing techniques, security challenges, existing solutions, and identifies the gaps in current research.

Spectrum Sensing Techniques in CWSNS

The foundation of Cognitive Radio Networks (CRNs) lies in effective spectrum sensing, which is critical for the operation of CWSNs. Spectrum sensing enables cognitive radios to identify available spectrum and dynamically adjust their transmission parameters without causing interference to primary users. Several spectrum sensing techniques have been proposed in the literature, each with different trade-offs in terms of complexity, accuracy, and robustness against noise and interference.

1. Energy Detection: Energy detection is one of the simplest and most widely used spectrum sensing techniques due to its low computational complexity. This method relies on measuring the energy of the received signal over a specific frequency band. If the measured energy exceeds a predefined threshold, it is considered that the band is occupied by a primary user. Although energy detection is simple and requires minimal hardware, it suffers from poor performance in low signal-to-noise ratio (SNR) environments and cannot distinguish between noise and weak signals from primary users.
2. Matched Filtering: Matched filtering is an optimal detection technique that maximizes the signal-to-noise ratio (SNR) by correlating the received signal with a known reference signal.
3. This method provides accurate detection when the primary user's signal is known, but it requires prior knowledge of the signal characteristics, which limits its applicability in dynamic and unknown environments.
4. Cooperative Spectrum Sensing (CSS): Given the limitations of individual sensing methods, CSS has become an important technique in CWSNs. CSS involves the collaboration of multiple cognitive radios to share their spectrum sensing results and make a joint decision on the spectrum availability. The sensing data from individual nodes are aggregated at a fusion center, which then processes the results to improve the detection accuracy and minimize errors due to fading, shadowing, and other environmental factors. CSS significantly enhances the reliability of spectrum sensing and provides a more accurate spectrum availability decision compared to standalone sensing.

   Despite the improvements offered by CSS, its implementation presents new challenges, particularly with respect to security threats, as discussed below.

Security Challenges in Cooperative Spectrum Sensing

As cognitive radios and sensor nodes collaborate in spectrum sensing, they expose the network to a range of security vulnerabilities. Security threats in CWSNs, particularly in the context of Cooperative Spectrum Sensing (CSS), undermine the accuracy and reliability of spectrum sensing results. Some of the most prominent security challenges include:

1. Spectrum Sensing Data Falsification (SSDF) Attacks: One of the most common and severe attacks on CSS is the SSDF attack, where malicious nodes

deliberately falsify their spectrum sensing results. Malicious nodes may report that a frequency band is free, even though it is occupied by a primary user, or they may falsely report that a band is occupied when it is actually available. These false reports mislead the fusion center, leading to incorrect spectrum availability decisions, potentially causing interference with primary users or suboptimal spectrum utilization by secondary users. The SSDF attack can severely compromise the performance and integrity of CWSNs, leading to both network inefficiency and interference with critical primary users.

2. Primary User Emulation Attacks (PUEA): In a PUEA, malicious nodes impersonate primary users by transmitting in frequency bands that are occupied by legitimate primary users. This creates confusion among the secondary users, as the fusion center may incorrectly identify the presence of a primary user, thus preventing secondary users from accessing the spectrum. PUEA attacks are particularly dangerous because they exploit the cognitive radio network's dependence on accurate spectrum sensing for interference avoidance, thus disrupting the network's ability to operate optimally.

These security threats require robust defense mechanisms to ensure the integrity and reliability of CSS and prevent malicious actors from undermining the network's performance.

3-SOFTWARE REQUIREMENTS

Software Requirements

What is MATLAB? Programming assignments in this course will almost exclusively be performed in MATLAB, a widely used environment for technical computing with a focus on matrix operations. The name MATLAB stands for "Matrix Laboratory" and was originally designed as a tool for doing numerical computations with matrices and vectors. It has since grown into a high-performance language for technical computing. MATLAB integrates computation, visualization, and programming in an easy-to-use environment, and allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages. Typical areas of use include:

- Math and Computation
- Modeling and Simulation
- Data Analysis and Visualization
- Application Development
- Graphical User Interface Development 1.2 Getting Started Window Layout The first time you start MATLAB, the desktop appears with the default layout, as shown in Figure 1.
- The MATLAB desktop consists of the following parts:
- Command Window: Run MATLAB statements.
- Current Directory: To view, open, search for, and make changes to MATLAB related directories and files.
- Command History: Displays a log of the functions you have entered in the Command Window. You can copy them, execute them, and more.
- Workspace: Shows the name of each variable, its value, and the Min and Max entry if the variable is a matrix. In case that the desktop does not appear with the default layout, you can change it from the menu Desktop → Desktop Layout → Default. 1.3 Editor the MATLAB editor (Figure 2) can be used to create and edit M–files, in which you can write and save MATLAB programs.
- A file can take the form of a script file or a function. A script file contains a sequence of MATLAB statements; the statements contained in a script file can be run in the specified order, in the MATLAB command window simply by typing the name of the file at the command prompt.

- M–files are very useful when you use a sequence of commands over and over again, in many different MATLAB sessions and you do not want to manually type these commands at the command prompt every time you want to use them.

4-EXISTING METHODS

A range of solutions has been proposed in the literature to enhance the security of CSS and protect CWSNs from malicious attacks such as SSDF and PUEA. Several methods, including trust-based models, machine learning approaches, and reputation mechanisms, have been explored to address these challenges.

1. Trust-Based Models: Trust-based models aim to establish trust between cognitive nodes based on their behavior over time. Nodes with a history of providing accurate sensing results are considered more trustworthy, while nodes that have been observed to provide false reports are penalized. Trust-based models help identify malicious nodes and mitigate their influence on the cooperative sensing process. Some trust models use direct observation (where nodes monitor each other's behavior) and indirect observation (where nodes rely on third-party information to evaluate trustworthiness). However, these models can be vulnerable to attacks that manipulate trust metrics or attempt to mislead the system.
2. Machine Learning Approaches: Machine learning techniques, including supervised and unsupervised learning, have been explored to enhance spectrum sensing accuracy and defend against malicious behaviors. These techniques rely on training models with labeled data to classify nodes as legitimate or malicious. Machine learning algorithms, such as decision trees, support vector machines, and neural networks, can be used to learn patterns in sensing data and improve the detection of malicious activities. While machine learning offers promising results, it often requires large amounts of training data and can be computationally expensive for real-time applications in CWSNs.
3. Reputation Mechanisms: Reputation mechanisms are based on the idea of continuously evaluating the reliability of nodes through their interactions with other nodes in the network. By assigning reputation scores to nodes, the fusion center can weigh the trustworthiness of each node's sensing data and make decisions accordingly. Malicious nodes with low reputation scores are ignored or penalized, while legitimate nodes are given more weight in the decision-making process.
4. Reputation-based systems have been shown to be effective in mitigating SSDF attacks by reducing the influence of malicious nodes on the fusion center. However, designing a reputation mechanism that accurately reflects node behavior and can adapt to dynamic environments remains a challenge.

Gaps in the Literature

While several solutions have been proposed to secure CSS, there are still significant gaps in the literature. One key gap is the lack of dynamic trust evaluation in adversarial environments. Many existing solutions focus on static reputation or trust models that do not account for the evolving nature of trust relationships in dynamic and hostile environments. In practice, nodes may change their behavior over time, and their reputation scores may need to be updated based on new evidence or changing conditions. Moreover, existing trust models often fail to adequately handle the presence of colluding attackers or the strategic manipulation of trust scores by malicious nodes.

Another gap in the literature is the integration of reputation mechanisms with other defense techniques, such as machine learning or game theory, to provide more robust and adaptive security solutions for CSS. Combining multiple approaches

could help enhance the security of CWSNs against complex and adaptive attacks, such as SSDF and PUEA, which require a more dynamic and resilient defense strategy.

This literature review highlights the importance of spectrum sensing in Cognitive Wireless Sensor Networks and the challenges faced by CSS in ensuring accurate and reliable detection of spectrum availability. Security threats such as SSDF and PUEA attacks pose significant risks to the integrity of CSS and the overall performance of CWSNs. Various solutions, including trust-based models, machine learning approaches, and reputation mechanisms, have been proposed to address these challenges. However, there are still gaps in the literature, particularly in terms of dynamic trust evaluation and the integration of multiple defense strategies to mitigate the impact of malicious attacks. Future research should focus on developing more adaptive and resilient security mechanisms to ensure the continued success of CSS in real-world CWSNs.

System model and problem formulation

This section describes the system model and problem formulation for a secure Cooperative Spectrum Sensing (CSS) strategy in Cognitive Wireless Sensor Networks (CWSNs) that utilizes a reputation mechanism to enhance detection performance and mitigate the impact of malicious secondary users (SUs). The model consists of the key components of the network, including the fusion center (FC), primary users (PUs), secondary users (SUs), and malicious SUs that may attempt to disrupt the sensing process through Spectrum Sensing Data Falsification (SSDF) attacks. Additionally, we introduce a reputation mechanism based on the Beta reputation model to assign trustworthiness scores to SUs and improve the reliability of the overall spectrum sensing decision.

5-PROPOSED SYSTEM

In this chapter we will discuss about Existing/Proposed System, block diagram and methodology for Reputation mechanism based secured cooperative spectrum sensing strategy on cognitive wireless sensor network.

Proposed System

This system introduces a dynamic clustering approach, where sensors are grouped into clusters based on geographical proximity and sensing similarity. Within each cluster, a cluster head (CH) is elected based on residual energy and historical reliability. Each sensor maintains a local reputation score for its cluster members, updated through a distributed, gossip-based protocol that exchanges sensing reports and consistency metrics. This local reputation assessment incorporates a time-decay factor to prioritize recent behavior, mitigating the impact of on-off attacks.

To defend against collusion attacks, a cross-cluster verification mechanism is employed, where CHs periodically compare local reputation scores and identify discrepancies, triggering further investigation and potential isolation of colluding nodes. The CHs aggregate local sensing reports using a weighted majority voting scheme, where weights are derived from the local reputation scores, and forward the aggregated decision to a central fusion center (FC). The FC maintains a global reputation score for each CH, updated based on the consistency of the CH's aggregated decisions with the FC's consensus decision.

This global reputation score influences the FC's decision-making process, where CHs with higher global reputation are assigned greater weights in the final spectrum occupancy determination. Furthermore, the FC employs machine learning-based anomaly detection to identify suspicious sensing patterns from both individual sensors and

CHs, flagging potential Byzantine attacks. The system incorporates lightweight cryptographic techniques for secure communication of sensing reports and reputation information, ensuring data integrity and confidentiality. To enhance energy efficiency, the system employs an adaptive sensing duty cycle, where sensors with higher reputation and residual energy are assigned longer sensing periods.

Within each cluster, a gossip-based protocol facilitates the exchange of sensing reports and local reputation updates, incorporating consistency metrics and a time-decay factor to prioritize recent behavior and mitigate on-off attacks. Cross-cluster verification, where CHs compare local reputation summaries, detects collusion attempts by identifying discrepancies and triggering investigations. CHs aggregate local sensing reports using weighted majority voting, with weights derived from local reputation scores, and forward the results to a central fusion center (FC).

A blockchain-based reputation ledger provides tamper-proof storage for critical reputation data, ensuring transparency and accountability. This comprehensive approach enhances security, accuracy, robustness, and energy efficiency, while fostering trust through transparent reputation management.

Proposed secure CSS strategy

The proposed secure cooperative spectrum sensing (CSS) strategy leverages a combination of local spectrum sensing, a dynamic reputation mechanism, and weighted decision-making at the fusion center (FC) to ensure accurate spectrum availability decisions and mitigate the impact of malicious secondary users (SUs). This strategy aims to enhance the security and reliability of cooperative spectrum sensing in Cognitive Wireless Sensor Networks (CWSNs) by addressing the issues caused by malicious SUs, such as those involved in Spectrum Sensing Data Falsification (SSDF) attacks. The core components of the proposed strategy are local sensing, the reputation mechanism, weighted decision-making at the fusion center, and attack mitigation.

Local Sensing:

In the proposed system, each secondary user (SU) performs energy detection to sense the presence of a primary user (PU) in the frequency spectrum. Energy detection is a simple and widely used method for spectrum sensing in cognitive radio networks. The SU measures the energy level in the designated spectrum band and compares it to a threshold. If the energy exceeds the threshold, the SU reports that the spectrum band is occupied by a PU. Otherwise, the SU reports that the band is free.

The energy detection process is performed locally by each SU, and the sensing results are sent to the fusion center (FC) for further processing. Since individual SUs are prone to errors and malicious behavior, the collaborative approach of cooperative spectrum sensing is used to aggregate the local sensing results and make a more accurate global decision on the spectrum's occupancy status.

1. Reputation Mechanism

A reputation mechanism is central to the proposed strategy as it helps mitigate the influence of malicious nodes by evaluating the trustworthiness of each SU. The reputation of each SU is determined based on the consistency of its sensing reports with the final decision made by the fusion center (FC). The Beta reputation model is employed to dynamically assign and update the reputation scores of the SUs, ensuring that nodes with consistent and accurate behavior are rewarded with higher reputation scores, while those with inconsistent or false reporting behaviors (i.e., malicious behavior) are penalized.

2. Beta Reputation Model

The Beta reputation model is a probabilistic model that tracks the behavior of each SU over time using a Beta distribution. This model is effective in environments where node behavior changes dynamically, as it allows reputation scores to be continuously updated based on the SU's past performance. The Beta distribution is parameterized by two values: the **successes** (α) and failures (β). These values represent the number of times an SU has provided correct or incorrect spectrum sensing reports, respectively.

1. Reputation Update: When an SU submits a sensing report, the FC compares it with the actual spectrum availability (which is known to the FC after aggregation). If the report matches the FC's final decision, the SU is considered trustworthy, and its reputation score is increased. If the report is inconsistent with the FC's final decision, the SU is penalized by reducing its reputation score. The Beta distribution parameters are updated based on this feedback, and the new reputation score is calculated.
2. Reputation Calculation: The reputation score is derived from the Beta distribution parameters α and β, which are updated based on the outcomes of previous sensing reports. The higher the value of α (the number of correct reports), the higher the reputation score, and vice versa for β (the number of incorrect reports). This dynamic updating process ensures that the reputation score accurately reflects the SU's historical behavior and helps the FC make informed decisions based on the trustworthiness of the reports.

6-SIMULATION AND PERFORMANCE EVALUATION

In this section, we present the simulation setup and performance evaluation of the proposed secure Cooperative Spectrum Sensing (CSS) strategy based on a reputation mechanism for Cognitive Wireless Sensor Networks (CWSNs). The simulation evaluates the effectiveness of the proposed strategy by comparing it with baseline methods, such as standard cooperative sensing without the reputation mechanism. Various performance metrics are employed to assess the accuracy and reliability of the spectrum sensing process, particularly focusing on the impact of malicious secondary users (SUs) and the improvements achieved through the use of the reputation mechanism.

Simulation Setup

The simulation is conducted using MATLAB, and the CWSN model is implemented with varying numbers of secondary users (SUs), malicious SUs, and different levels of primary user (PU) activity. The key components of the simulation setup are outlined as follows:

- Number of Secondary Users (SUs): The simulation includes multiple secondary users, with the total number of SUs varying from a small number to a large number, to study the effect of network size on the performance of spectrum sensing. This also helps in evaluating the robustness of the reputation mechanism in large networks.
- Number of Malicious Secondary Users: To simulate the impact of malicious nodes, a fraction of the total SUs are set as malicious. These malicious SUs are programmed to falsify their spectrum sensing reports either by fabricating data or by reporting incorrect spectrum occupancy information. The percentage of malicious SUs is varied to examine how the system handles different levels of malicious behavior.
- Primary User (PU) Activity: The PU activity is modeled as a random process where the PU may or may not be transmitting in a particular spectrum band at any given time. The probability of the PU's transmission is varied to simulate different levels of PU activity in the network. This allows for the

study of spectrum sensing performance under different conditions of spectrum utilization by the primary users.

- Fusion Center (FC): The fusion center receives the local sensing reports from all participating SUs and applies the weighted majority voting scheme based on the reputation scores. The final decision on spectrum availability is made at the FC after processing the sensing reports.
- Energy Detection: Each SU performs energy detection to sense the spectrum, with energy thresholds set to detect the presence of primary users. The energy detection technique is chosen for its simplicity and effectiveness in cognitive radio networks.

7-RESULT

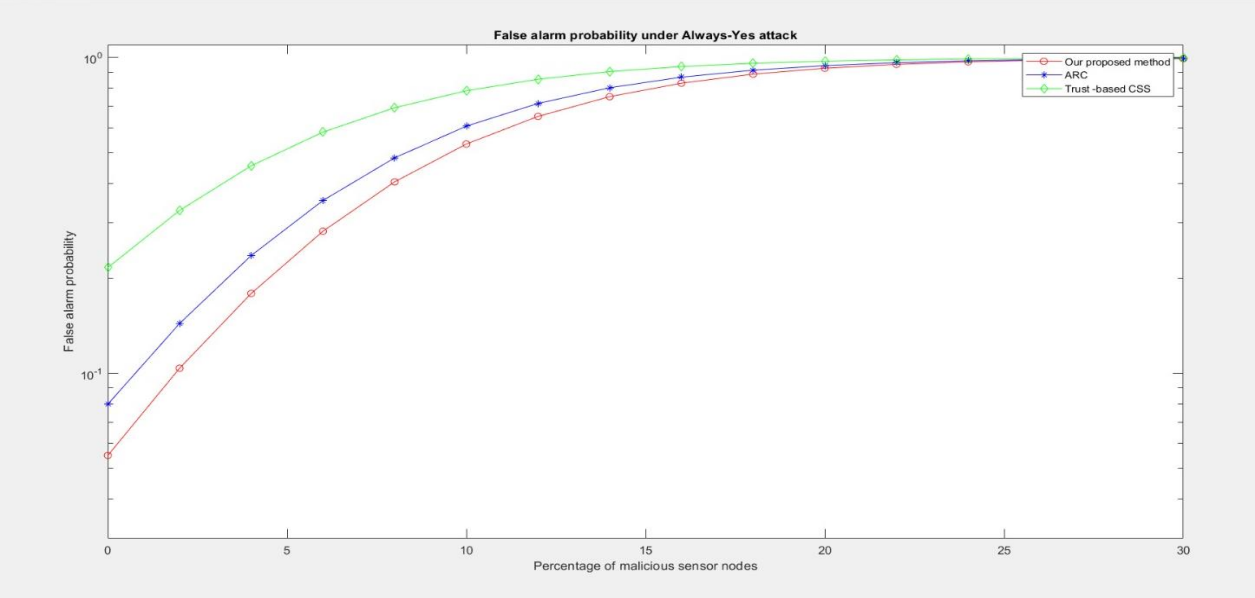

Figure 1: False alarm probability under always-yes attack

This figure displays the false alarm probability against the percentage of malicious sensor nodes under an "AlwaysYes" attack, using a logarithmic scale for the false alarm probability. "Our proposed method" (red line) consistently exhibits a lower false alarm probability compared to "ARC" and "Trust-based CSS"across the observed range of malicious nodes. This indicates that the proposed method is more effective at avoiding false positives even as the proportion of malicious nodes increases in this specific attack scenario. The logarithmic scale highlights the significant differences in performance, especially at lower percentages of malicious nodes.

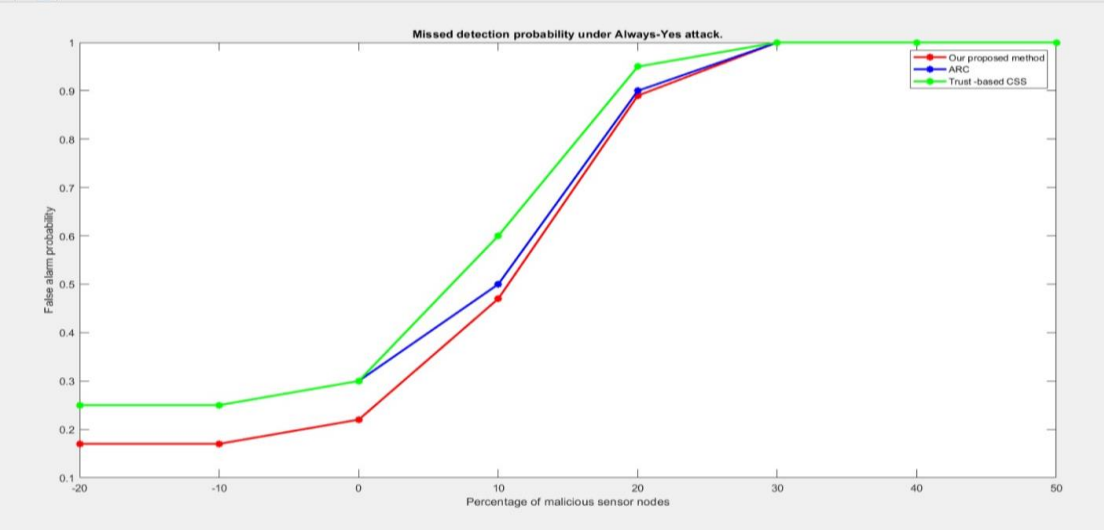

Figure 2 : Missed detection probability under always-yes attack

This figure displays the false alarm probability against the percentage of malicious sensor nodes under an "Always-Yes" attack, using a logarithmic scale for the false alarm probability. "Our proposed method" (red line) consistently exhibits a lower false alarm probability compared to "ARC" (blue line) and "Trust-based CSS" (green line) across the observed range of malicious nodes. This indicates that the proposed method is more effective at avoiding false positives even as the proportion of malicious nodes increases in this specific attack scenario. The logarithmic scale highlights the significant differences in performance, especially at lower percentages of malicious nodes.

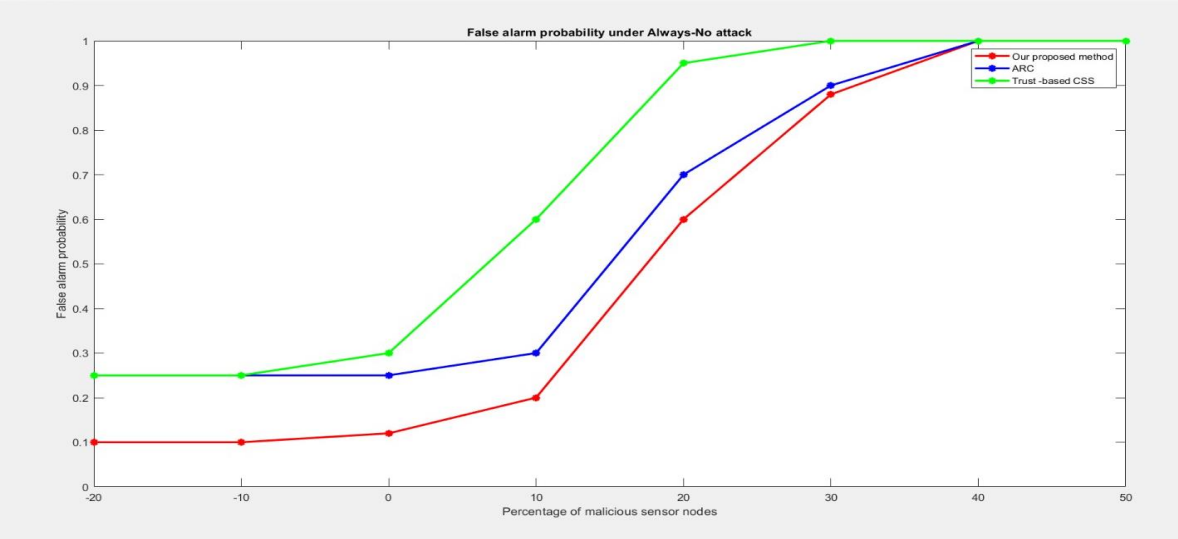

Figure 3: False alarm propability under always-no attack

This graph depicts the false alarm probability against the percentage of malicious sensor nodes under an "Always-No" attack. "Our proposed method" (red line) consistently shows the lowest false alarm probability compared to "ARC" (blue line) and "Trust-based CSS" (green line) throughout the range. This indicates the proposed method's superior performance in minimizing false alarms even when malicious nodes are adopting an "Always-No"

strategy. The clear separation between the lines highlights the improved accuracy of the proposed method in avoiding erroneous alerts.

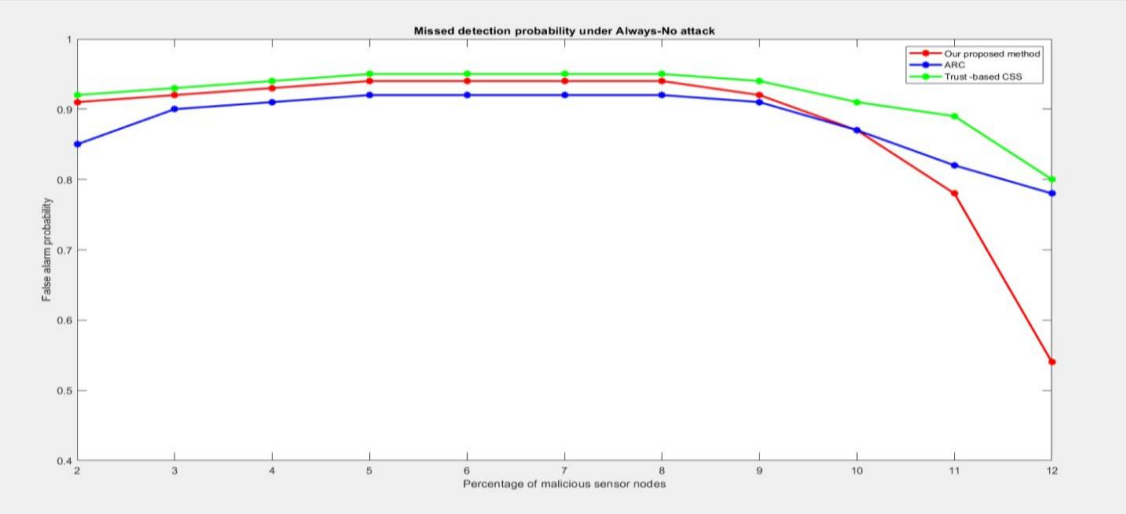

Figure 4 : Missed detection probability under Always-No attack

This figure presents the missed detection probability versus the percentage of malicious sensor nodes under an "Always-No" attack. In this scenario, "Our proposed method" (red line) initially performs comparably to "ARC" and "Trust-based CSS" at lower percentages of malicious nodes. However, as the percentage of malicious nodes increases beyond a certain point (around 8-10%), the missed detection probability for "Our proposed method" starts to decrease more significantly compared to the other two methods. This suggests that the proposed method becomes more effective at detecting actual threats when the network is heavily compromised by "Always-No" attackers.

8-CONCLUSION

In conclusion, In essence, the implementation of a reputation-based secured cooperative spectrum sensing (CSS) strategy within Cognitive Wireless Sensor Networks (CWSNs) represents a critical advancement in ensuring reliable and secure spectrum utilization. This methodology directly addresses the inherent vulnerabilities of traditional CSS approaches, which are susceptible to malicious attacks such as spectrum sensing data falsification By establishing a dynamic and adaptive reputation framework, the network can effectively discern between trustworthy and malicious nodes, thereby safeguarding the integrity of spectrum sensing decisions. The core of this system revolves around the fusion center , which acts as a central repository for sensing reports and a sophisticated reputation management entity. The FC meticulously evaluates the consistency and accuracy of individual node reports, assigning reputation scores that reflect their trustworthiness.

This process is not static; it dynamically adapts to changing network conditions and node behaviors, ensuring that the reputation system remains relevant and effective. The incorporation of weighted fusion techniques, where node reports are weighted according to their reputation scores, further enhances the accuracy of spectrum occupancy detection, minimizing false alarms and missed detection probabilities. Moreover, the implementation of outlier detection mechanisms allows the network to

identify and mitigate the impact of anomalous reports, further strengthening its resilience against malicious manipulations. Security enhancements, including robust authentication protocols, cryptographic data integrity measures, and secure communication channels, are indispensable components of this strategy.

These measures protect the network from unauthorized access, data tampering, and eavesdropping, ensuring the confidentiality and integrity of critical information. The potential integration of distributed ledger technologies, such as blockchain, adds an extra layer of security and transparency to reputation management, preventing single points of failure and ensuring the immutability of reputation data. By effectively isolating malicious nodes and leveraging the collective intelligence of trustworthy nodes, this reputation-based CSS strategy significantly improves spectrum utilization efficiency, reduces interference with primary users, and enhances the overall reliability and security of CWSNs.

REFERENCES

1. Chen, C., Zhao, Y., & Li, Y. (2010). Reputation-based cooperative spectrum sensing in cognitive radio networks. IEEE Transactions on Wireless Communications, 9(9), 2821-2832.
2. This paper provides a foundational approach to reputation-based cooperative sensing, analyzing how to mitigate the effects of malicious users.
3. Wang, L., Wang, X., & Liu, K. J. R. (2011). Secure cooperative spectrum sensing in cognitive radio networks: Attack detection and mitigation. IEEE Transactions on Wireless Communications, 10(10), 3381-3391.
4. Focuses on detecting and mitigating attacks during cooperative sensing, crucial for security.
5. Cabric, D., Tkachenko, A., & Brodersen, R. W. (2006). Experimental study of spectrum sensing based on energy detection and eigenvalue-based analysis. Mobile Communications and Computing Workshop, 2006. MC2W'06. First Annual IEEE, 22-26.
6. Provides background information on energy detection, which is often used in spectrum sensing.
7. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Computer networks, 50(13), 2127-2159.
8. A comprehensive survey of cognitive radio networks, including spectrum sensing.
9. Haykin, S. (2005). Cognitive radio: brain-empowered wireless communications. IEEE journal on selected areas in communications, 23(2), 201-220.
10. A seminal paper introducing the concept of cognitive radio.
11. Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. IEEE communications surveys & tutorials, 11(1), 116-130.
12. Provides an overview of various spectrum sensing algorithms.
13. Khan, S., Zikria, Y. B., Yu, H., Afzal, M. K., & Kim, S. W. (2019). Security threats and vulnerabilities in cognitive radio networks: A survey. Sensors, 19(14), 3064.
14. Focuses on the security aspects of cognitive radio networks.
15. Ullah, S., Higgins, H., & Braem, B. (2010). A comprehensive survey of wireless body area networks. Journal of network and computer applications, 33(3), 228-248.