IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"Energy-Efficient Joint Spectrum Sensing And Power Allocation In Cognitive Iot Under SSDF Attack" Review Paper

Amisha Malviya[1], Mr. Amit Tripathi[2]
[1]Research Scholar, [2]Professor
Department of Electronics & Communication Engineering,
Technocrats Institute of Technology (Main),Bhopal, MP.

Abstract: Spectrum scarcity poses a critical challenge to the growing demand for wireless services. Cognitive Radio Networks (CRNs) address this issue by enabling secondary users (SUs) to opportunistically access licensed spectrum bands when they are unoccupied, without interfering with primary users (PUs). Through key functions such as spectrum sensing, analysis, mobility, and sharing, CRNs dynamically reconfigure network parameters to adapt to environmental conditions. Cooperative Spectrum Sensing (CSS), where multiple SUs share sensing information, improves detection reliability by mitigating the effects of fading and shadowing. However, the open and reconfigurable nature of CRNs makes them highly vulnerable to security threats, particularly Spectrum Sensing Data Falsification (SSDF) attacks, where malicious users (MUs) manipulate sensing results to gain unfair access or disrupt spectrum availability. Existing security mechanisms often fail to provide adequate robustness while maintaining low computational complexity, limiting their suitability for resource-constrained environments.

***Index Terms* -** Cognitive Radio Networks (CRN); Spectrum Sensing; Cooperative Spectrum Sensing (CSS); Spectrum Sensing Data Falsification (SSDF); Malicious Users (MU); Trust Management; Multifactor Trust; SETM Algorithm; Security; Complexity Analysis.

I. INTRODUCTION

Cognitive Radio (CR) technology represents a transformative approach in wireless communication that enables more efficient utilization of the radio frequency spectrum. Traditionally, frequency bands have been statically allocated to licensed or primary users (PUs), leading to significant underutilization. Studies have revealed that many licensed bands remain idle for a large portion of time, contributing to the so-called "spectrum scarcity paradox." Cognitive Radio resolves this issue through Dynamic Spectrum Access (DSA), a mechanism that allows CRs to intelligently sense, identify, and opportunistically utilize unoccupied portions of the licensed spectrum—commonly referred to as spectrum holes or white spaces—without causing interference to the Pus.

Through the **Cognitive Radio Network (CRN)** framework, multiple SUs coordinate to ensure fair, interference-free communication, thus optimizing overall spectrum utilization. Figure 1 depicts the diverse applications of CRN, including public safety networks, military communications, emergency response systems, and rural broadband access.

Cognitive Decision Engine (CDE): the **Cognitive Radio Network (CRN)** framework, multiple SUs coordinate to ensure fair, interference-free communication, thus optimizing overall spectrum utilization. Figure 1 depicts the diverse applications of CRN, including public safety networks, military communications, emergency response systems, and rural broadband access.

The wireless nature and reconfigurable characteristics of Cognitive Radios (CRs) make them highly vulnerable to security threats, thereby elevating security as a critical concern (Alexandros et al., 2013).

Threats occurring at the physical layer can disrupt the overall network operation, while those at the MAC layer can directly manipulate the spectrum sensing results of CRs. Hence, this thesis focuses on addressing MAC-layer security challenges and proposes solutions to mitigate these threats.

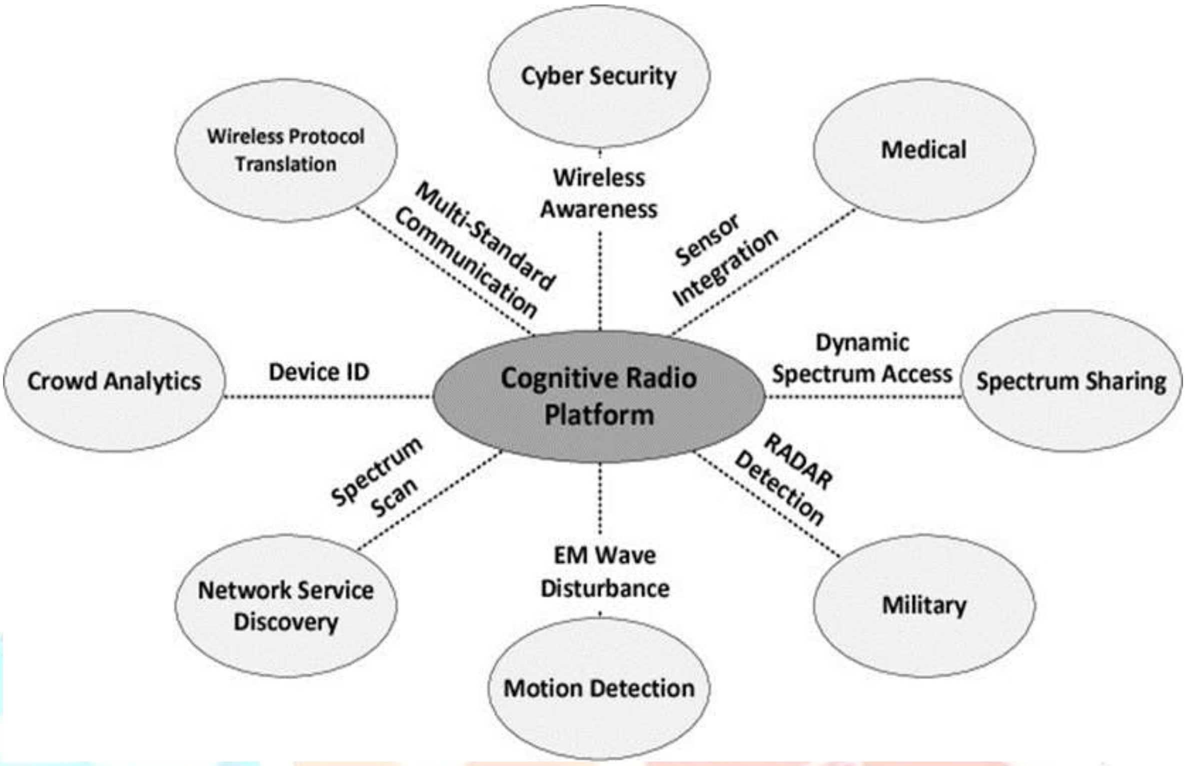

Figure -1 Applications of CRN

Cognitive Radio Network Architecture

A Cognitive Radio Network (CRN) is formed by the interconnection of multiple Cognitive Radios (CRs). Broadly, CRNs can be categorized into centralized (infrastructure-based) and distributed (ad hoc-based) architectures.

In a centralized CRN, the network is organized around a central node known as the Fusion Center (FC), which is responsible for controlling and managing the overall system. Conversely, a distributed CRN lacks infrastructure; CRs communicate directly with one another, and information is shared collaboratively without the requirement of a central control entity. The architectural models of both centralized and distributed CRNs are illustrated in Figure 2.

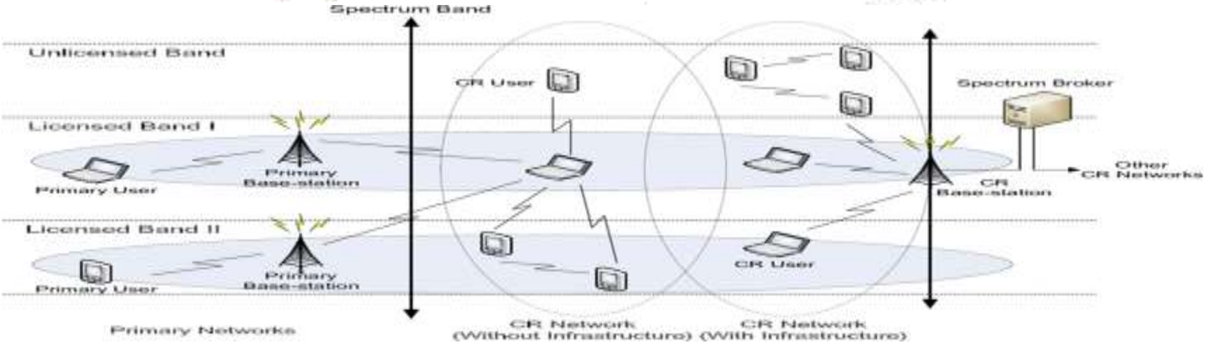

Figure-2 Architecture of CRN

II. OBJECTIVE

The main objectives of this research are:

To study and analyze the various security threats in Cognitive Radio Networks.

To propose an efficient multifactor trust model for combating the Spectrum Sensing Data Falsification (SSDF) attack.

To implement the proposed trust-based algorithm using logistic regression tree classifier, a supervised machine learning approach, for accurate detection of malicious users.
To evaluate and compare the performance of different supervised machine learning algorithms on the proposed multifactor trust model.

III. **LITERATURE REVIEW**

The aim of developing a multifactor trust-based security algorithm is to design a less complex yet more robust Cognitive Radio Network (CRN) against Spectrum Sensing Data Falsification (SSDF) attacks.
The literature survey for this work can broadly be divided into two categories:

A. Identifying malicious users (MUs) using machine learning (ML) algorithms.
B. Mitigating SSDF attacks using trust-based methodologies.

A. Machine Learning-Based Approaches for SSDF Detection in CRN Literature Review.

Zhang et al. (2025) Massive wireless connectivity demands in the Internet of Things (IoT) ecosystem necessitate significant spectrum resources. To address spectrum scarcity, Cognitive Radio-Enabled IoT (CR-IoT) has emerged as a viable solution. However, CR-IoT systems face major challenges, particularly spectrum sensing data falsification (SSDF) attacks during cooperative sensing and constraints on energy efficiency due to the limited power capabilities of IoT terminals. To address these issues, a joint spectrum sensing and secure power allocation scheme has been proposed, designed specifically to operate under SSDF attack conditions. The scheme incorporates a weighted data transmission time allocation mechanism based on trust degrees, which are dynamically updated using an online learning algorithm during power allocation. Furthermore, a joint optimization problem is formulated to maximize the CR-IoT system's energy efficiency by optimizing spectrum sensing time, the number of cooperative nodes, and transmission power.

Balachander **et al. (2024)** Recently, Cooperative Spectrum Sensing (CSS) in Cognitive Radio Networks (CRNs) has become a cornerstone for achieving efficient 5G wireless communication, particularly in support of Internet of Things (IoT) applications. Spectrum sensing is critical in CRNs for identifying and utilizing underused spectrum bands. CSS enhances this process through spatial diversity, leading to improved detection accuracy and reliability. As 5G technologies rapidly evolve to support the demands of next-generation IoT networks, CSS continues to gain attention due to its high-speed performance and robustness in dynamic environments.

Ernesto et al. (2020) focused on PUE attack detection using SVM, incorporating Renyi entropy and SNR features. The classifier distinguished genuine PUs using modulation-specific behavior learned via GMSK and OFDM. A Software Defined Radio (SDR) testbed validated the model’s real-world applicability.

Gul et al. (2020) used an AdaBoost-based Boosted Tree Algorithm (BTA) to detect multiple types of SSDF attackers. The BTA ensemble enhanced prediction by combining weak classifiers. Though effective, the study did not compare the proposed model against other ML algorithms for optimality.

Sarmah et al. (2020) examined supervised ML algorithms including Neural Networks (NN), SVM, Naïve Bayes, and Ensemble Classifiers. Datasets were prepared using frequency-based dibit grouping. NN and ensemble classifiers exhibited consistent and strong performance. However, selfish and alternator MU types were not addressed.

Zhu et al. (2018) employed Support Vector Machines (SVM) to evaluate SU behavior across multiple sensing rounds. The study provided a detailed mathematical formulation for misclassification probability and employed likelihood ratio tests for PU estimation. Though SVM performed robustly under adverse conditions, it did not address selfish MUs and lacked comparative evaluation against diverse ML models.

B. Mitigating SSDF attacks using trust-based methodologies Literature Review.

Rajorshi et al. (2020) proposed a reputation-based SSDF attack mitigation technique utilizing a Distributed Fusion Center (DFC) architecture. In this scheme, selected SUs act as DFCs and apply majority voting to assess sensing reliability. Weights are normalized for each SU, and reputation is updated based on the confidence of election, which increases if a majority decision is reached with a significant margin. The authors use a confidence-adaptive learning rate, where a constant learning rate is scaled by the election confidence level. The method successfully identifies always-yes, always-no, always-false, and random attackers, but cannot detect selfish MUs.

Guowei Zhang (2020) introduced a blockchain-based security mechanism to mitigate SSDF attacks in CRNs. The proposed method leverages both blockchain and reputation management, where reputation is computed in two phases: direct credibility, based on historical sensing data, and recommendation credibility, sourced from neighboring SUs. To prevent collusive attacks, blockchain is used as a distributed ledger that stores historic behaviors and interactions, ensuring transparency and immutability. The comprehensive reputation score, combining both direct and recommended evaluations, is used for final decision-making, improving robustness against false information propagation.

Yadav K. et al. (2020) introduced a modified delivery-based spectrum sensing system where only a minimal number of samples are used to determine spectrum occupancy in cognitive radio networks. In this method, a scheduled secondary user (SU) is permitted to transmit data based on the global decision made by the Fusion Center (FC). If the SU's transmission is successful, the global decision is considered valid; otherwise, it is deemed incorrect. Although this scheme focuses on minimizing sampling requirements, it lacks specific details on how the sample count is reduced and offers no clear mechanism for the identification of malicious users (MUs).

G. Rathe et al. (2019) developed a trust-based framework for detecting malicious users and securing the network against Primary User Emulation Attacks (PUEAs). Their approach includes a trusted routing and handoff mechanism, supported by a trust analyzer situated between the cognitive user (CU) and the network layer. This analyzer computes rating and trust values using the Social Impact Theory Optimizer, based on historical interactions and network positioning. Trust values are initially assigned randomly and updated using Tidal Trust Algorithm. Evaluation metrics include packet delivery ratio, delay, relative trust, true/false positive rates, and average authentication delay. The algorithm achieved an 88% success rate in simulation.

Adele et al. (2018) proposed a trust-based scheme for multi-hop cooperative spectrum sensing in distributed cognitive radio networks (CRNs). In this framework, secondary users (SUs) broadcast their sensing reports to neighboring users within their transmission range. Each broadcast packet contains detailed information, including the SU's identity, channel number, channel status, and the trust value of the transmission path the packet traverses.

IV. METHODOLOGY FOR SIFTING AND EVALAUTION TRUST MANAGEMENT ALGORITHM

The security of Cognitive Radio Networks (CRNs) is critical, as various threats can disrupt their core functionalities. Among these, the Spectrum Sensing Data Falsification (SSDF) attack is particularly severe, as it directly targets the fundamental function of CRNs spectrum sensing. If sensing results are falsified, the entire purpose of the CRN is compromised. Therefore, developing an effective solution to counter SSDF attacks is of great importance.

PROPOSED SETM SCHEME

The proposed model consists of K SUs that sense the spectrum within a time slot T, along with M MUs employing different attacking strategies. The CRN is modeled as a centralized system, where the Fusion Center (FC) acts as the most powerful and trusted entity with significant processing capabilities.

The system assumes ideal control channel conditions, ensuring error-free transmission between the FC and SUs. Each SU employs energy detection to determine the presence or absence of a Primary User (PU). Additionally, path loss is neglected since the CRN's coverage area is considered relatively small (Praveen

Kaligineedi et al., 2008). Cooperative Spectrum Sensing (CSS) is employed as the communication mechanism between the FC and SUs.

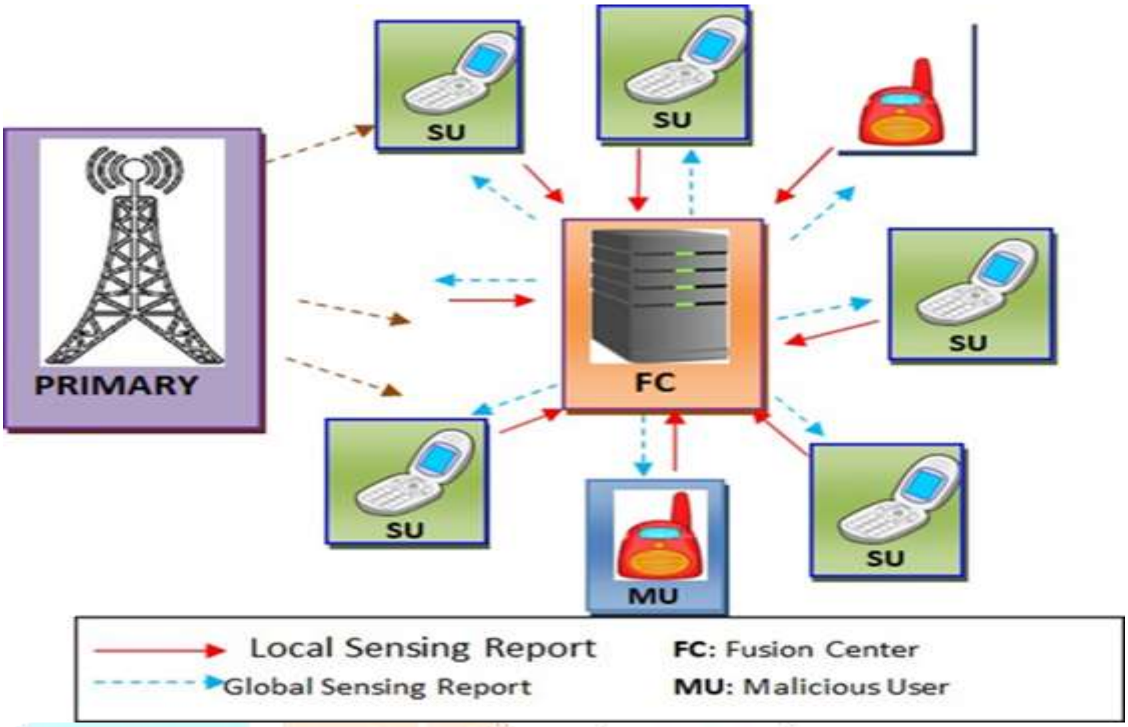

Fig-3 Spectrum Sensing of SU

The detection of Primary Users (PUs) in a CRN is carried out by the Fusion Center (FC) based on hypothesis testing. The process can be mathematically formulated as:

$$H_0: Y_S(k) = w_s(k) \quad H_1: Y_S(k) = w_s(k) + h_{SP}(k)P(k)$$

where:
$Y_S(k)$ denotes the received signal of the k^{th} SU,
$w_s(k)$ is the Additive White Gaussian Noise (AWGN) with zero mean and variance σ^2,
$P(k)$ represents the PU signal sample detected by the k^{th} SU,
$h_{SP}(k)$ is the complex channel gain between the PU and the k^{th} SU.
The FC combines the sensing results from all K SUs to make the final decision:

$$F_K = \sum_{k=1}^{K} Y^2(k)$$

The FC adopts the hard decision rule with majority voting, which is both bandwidth-efficient and simple to implement. Each SU sends a binary decision “1” for PU presence and “0” for PU absence. The FC then decides in favor of the hypothesis supported by at least K out of S SUs.
Thus, the decision rules can be expressed as:

$$H_0: \sum_{k=1}^{K} Y^2(k) < K \quad \Rightarrow \text{PU absent} \quad H_1: \sum_{k=1}^{K} Y^2(k) \geq K \quad \Rightarrow \text{PU present}$$

FC Record Table

Time slots / SUs	SU_1^r	SU_2^r	SU_3^r	SU_4^r	SU_5^r	SU_6^r	SU_7^r	…	SU_s^r	FCO
ts_0	1	0	1	1	0	1	1	…	1	1
ts_1	1	1	0	X	0	0	0	…	1	0
ts_2	1	0	1	1	0	1	0	…	X	1
…	…	…	…	…	…	…	…	…	…	…
ts_k	1	1	0	1	0	0	0	…	0	0

Table-1

Here:

X represents a missing sensing report from an SU.

FCO denotes the final cooperative output of the FC, determined using the K-out-of-N rule.

From the table:

Rows represent the sensing outcomes of all SUs at different time slots.

Columns correspond to the sensing history of each SU across time slots

V. RESULTS AND DISCUSSION

Table-2 illustrates the variation of past event trust, requite trust, reliability trust, and cumulative trust with increasing percentages of malicious behavior in SUs. The registry trust remains constant at ‘1’ under the assumption that each SU provides all its sensing results to the FCO within the prescribed time slots.

The results show that:

When a SU exhibits 10% malicious behavior (i.e., only one false report), the cumulative trust is relatively high at 1.676.

As the percentage of malicious reporting increases from 20% to 90%, the cumulative trust decreases steadily, from 1.434 to -0.264.

Sl. No	Percentage of Malicious Behavior	Past Event Trust	Registry Trust	Requite Trust	Reliability Trust	Cumulative Trust
1	10%	8.5	1	0.9	0.90	1.676
2	20%	6.5	1	0.8	0.86	1.434
3	30%	4.5	1	0.7	0.84	1.196
4	40%	2.5	1	0.6	0.83	0.958
5	50%	0.5	1	0.5	0.83	0.716
6	60%	-1.5	1	0.4	-0.83	0.502
7	70%	-3.5	1	0.3	-0.84	0.176

Sl. No	Percentage of Malicious Behavior	Past Event Trust	Registry Trust	Requite Trust	Reliability Trust	Cumulative Trust
8	80%	-5.5	1	0.2	-0.86	-0.046
9	90%	-7.5	1	0.1	-0.90	-0.264

Table-2

ANALYSIS OF RESULTS

The results show that:
When a SU exhibits 10% malicious behavior (i.e., only one false report), the cumulative trust is relatively high at 1.676.
As the percentage of malicious reporting increases from 20% to 90%, the cumulative trust decreases steadily, from 1.434 to -0.264.
This demonstrates a negative correlation between malicious behavior and trust: as the maliciousness of an SU increases, its trustworthiness declines.

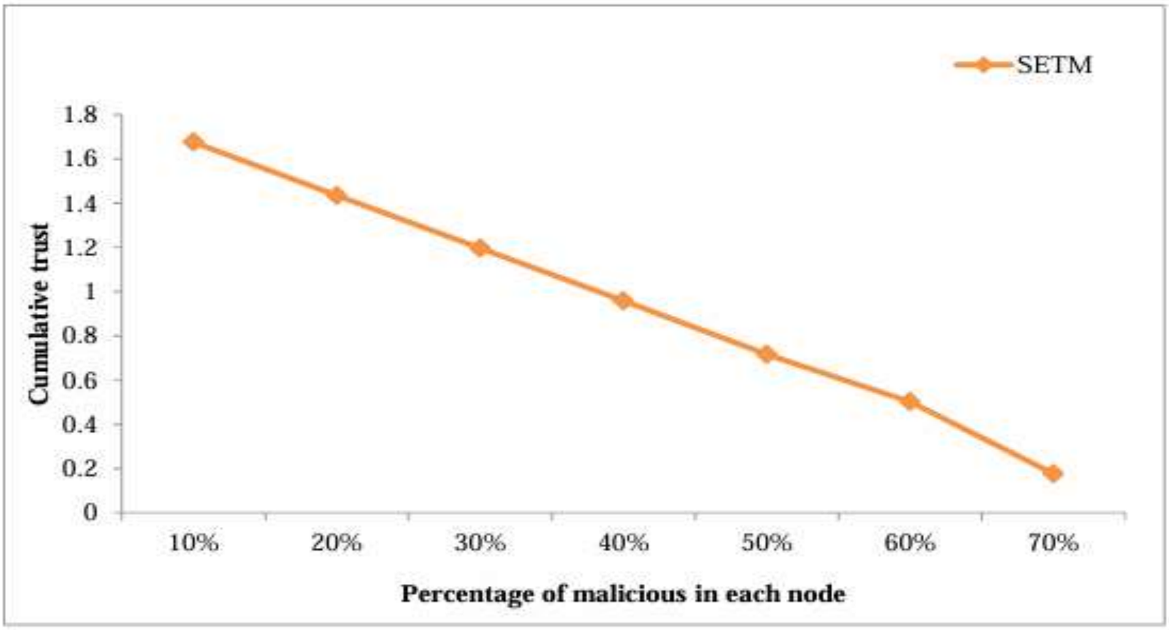

Fig-4 Comparison of Cumulative Trust with the variation in the malicious behavior of SU

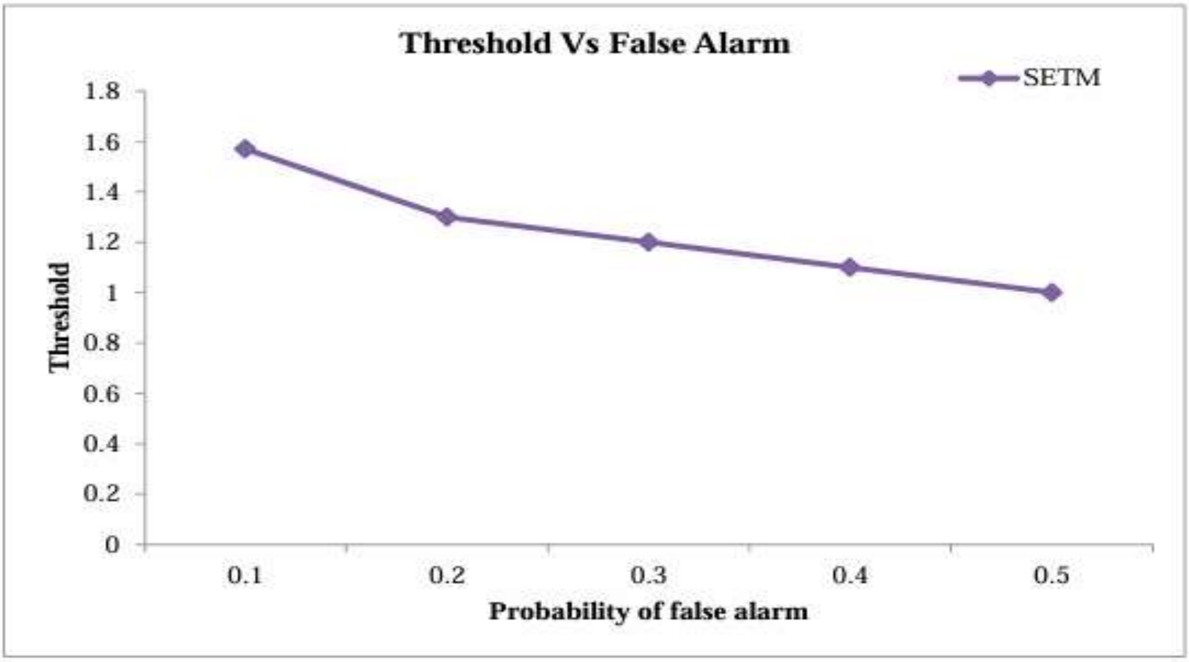

Fig-5 Variation of the Threshold with Probability of False Alarm

VI. CONCLUSIONS

The rapid growth of wireless communication technologies combined with static spectrum allocation policies has led to the pressing issue of spectrum scarcity. Cognitive Radio Networks (CRNs) address this challenge by allowing Secondary Users (SUs) to opportunistically utilize the licensed spectrum of Primary Users (PUs) when not in use. However, the efficiency of spectrum utilization in CRNs critically depends on the accuracy of spectrum sensing, particularly under Cooperative Spectrum Sensing (CSS). CSS, while effective, is highly vulnerable to Spectrum Sensing Data Falsification (SSDF) attacks, which degrade the reliability and security of the network.

Although multiple security mechanisms have been proposed to counter SSDF attacks, achieving low computational complexity, high robustness, reduced overhead, and uncompromised security remains a significant challenge. This research work addresses these challenges by proposing a multifactor trust-based security framework supported by Machine Learning (ML) techniques, focusing on identifying and mitigating all categories of SSDF attackers.

VII. REFERENCES

Wang, W., Zhang, X., & Guo, D. (2009). *Journal of Computational Information Systems*, 5(6), 1803–1810.

Rawat, A. S., Anand, S., & Subbalakshmi, K. P. (2010). Countering collaborative spectrum sensing attacks using reputation system. *In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–5.

Arshad, R., & Lenhart, K. (2011). A robust reputation-based scheme for spectrum sensing in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking*, 2011(1), 1–11. https://doi.org/10.1186/1687-1499-2011-210

Feng, W., Zhang, Y., Qin, Z., & Li, Y. (2013). Sensing guard: A trust-based security architecture for collaborative spectrum sensing in cognitive radio networks. *Wireless Networks*, 19(4), 685–700. https://doi.org/10.1007/s11276-012-0516-1

Zeng, K., Li, P., Shu, Y., & Fang, Y. (2010). Secure collaborative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 9(6), 2030–2040. https://doi.org/10.1109/TWC.2010.06.090349

Praveen, B., & Venkatesh, K. (2010). Outlier detection approach for identifying malicious users in cooperative spectrum sensing. *In Proceedings of the IEEE International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1–6.

Hyder, C., Akbar, M., & Sher, M. (2014). Adaptive reputation-based clustering against SSDF attacks in cooperative spectrum sensing. *EURASIP Journal on Wireless Communications and Networking*, 2014(1), 1–9. https://doi.org/10.1186/1687-1499-2014-165

Bansal, T., Chen, J., & Sethi, A. (2014). Fast probe: Malicious user detection in cognitive radio networks through active transmissions. *IEEE Transactions on Mobile Computing*, 13(8), 1801–1814. https://doi.org/10.1109/TMC.2013.100

Sucasas, V., Costa-Perez, X., & Vidal, J. (2015). Lightweight and secure spectrum sensing for cognitive radio networks. *IEEE Transactions on Mobile Computing*, 14(10), 1942–1955. https://doi.org/10.1109/TMC.2014.2365186

Sharifi, A., Moghaddam, M. E., & Shokrollahi, S. (2016). Attack-aware cooperative spectrum sensing against spectrum sensing data falsification attack. *AEU - International Journal of Electronics and Communications*, 70(10), 1393–1402. https://doi.org/10.1016/j.aeue.2016.07.002