Al-Mukhtar Journal of Sciences 08 (1): 65-74, 2024
Doi: https://doi.org/10.54172/1jpfs115

Research Article Open Access

Robust Detection Technique in Cooperative Radio Networks

Mahmoud Ali Ammar[1], Abderazag Masoud[2] and Ali F. kaeib[3]

Corresponding author: M.ammar@zu.edu.ly, Department of Computer, Faculty of Computer Technology University of Zawia, Libya

[2, 3] Department of Computer, Faculty of Computer Technology, University of Zawia, Libya

Received:
21 September 2024

Accepted:
05 December 2024

Publish online:
31 December 2024

Abstract
Traditional spectrum management reserves most of the spectrum for licensed users with exclusive access. To address spectrum scarcity, it is crucial to explore unlicensed operations in licensed bands so the interference between the Primary Users (PU) and Secondary Users (SU) is prevented. The success of Cognitive Radio (CR) networks depends on robust security measures to avoid misuse and to ensure trust among nodes, requiring mechanisms to distinguish primary from secondary user signals. While secondary users enhance spectrum utilization by sensing and accessing available frequencies, this capability introduces security risks. Malicious users can exploit the system to disrupt operations and degrade frequency determination performance. To mitigate these issues, the proposed scheme integrates advanced security measures based on trust and weight values to ensure secure spectrum access. It evaluated the trustworthiness of each SU using location coordinates and received signal strength. SUs performs independent frequency determination and submit data to a Fusion Center (FC) The FC combines local sensing results with trust weights and applies some rules to detect primary user presence reliably. A Limited Threshold Range (LTR) mechanism is proposed to minimize the impact of low-trust users by reducing their influence on decision-making. The LTR ensures that users from the threshold value contribute less to the decision and the visa-versa. This approach leads to enhancing decision accuracy.

Keywords: Cognitive Radio, Primary Users, Secondary Users, Primary User Emulation Attack , Cooperative Spectrum Sensing, Frequency Determination, Fusion Center.

INTRODUCTION

Frequency determination and sharing free bands are crucial functions of cognitive radio that allow secondary nodes to access the free bands and to identify available spectrums to be occupied (Chen & Park, 2006). Along with these capabilities, addressing the security and reliability challenges within cognitive radio networks is essential. One example of cognitive radio application is using unused spectrum (often referred to as white spaces) in television bands, where the television transmitter serves as the master node and the TV frequency is used by the secondary users.

In a cognitive radio network, users are divided into two groups; group one is for the primary nodes, while the other is for the secondary nodes. The main purpose of frequency determination in such networks is to detect unused spectral frequencies, also referred to as "white spaces," to be used by

the cognitive radio nodes (Letaief & Zhang, 2009). In this step, the legitimate nodes have the chance to use the spectrum, while the other nodes must relinquish their turn of the spectrum if primary users need it with no interference occurring.

If a node starts transmitting on a frequency used by another secondary node, the secondary node is expected to leave the frequency quickly. However, when no primary user is actively communicating, all other users are permitted to access the unoccupied spectrum. In some cases, secondary users may attempt to copy the primary node information to have unauthorized access to the spectrum. This can lead to malicious behavior where secondary users are mistaken for primary users, causing other secondary users to vacate the spectrum for the malicious actor (Letaief & Zhang, 2009). A PUEA occurs when a lousy node uses the details of the signal of a primary node to occupy idle channels, thereby obstructing access to the spectrum. Such attacks can create significant problems in cognitive radio networks. PUEA can be initiated during frequency determination through various detection methods, including cyclostationary, energy, or matched filter detection techniques (Hossain & Bhargava, 2007). Among these, the based method is the most widely used.

This research proposes a Limited Threshold Range (LTR) approach to combat PUEA. The idea behind LTR is that the farther away a user is from the threshold, the more likely the correct decision is made. This technique helps prevent low-trust users from influencing the decision-making process regarding the PU and SU in the network.

Cooperative frequency determination can be employed to address the uncertainty inherent in frequency determination within CRN. Several techniques for cooperative frequency determination have been used. The simplest approach involves using OR or AND operations on the sensing results from multiple nodes. For another example, the maximal ratio combination has been explored (Simon & Alouini, 2005). A cooperation using a Likelihood Ratio Test was suggested by (Digham et al., 2003). (Ghasemi & Sousa, 2007) proposed a sensor technique for cooperative frequency determination to save energy, and (Akyildiz et al., 2011) suggested using fuzzy logic. However, a trust cooperative frequency determination method using a majority rule is introduced in our proposed scheme for CRN. In this approach, individual users conclude the local result about the PU status; thus, a Fusion Center concludes the overall result about the PU presence. This scheme enhances sensing accuracy while conserving the energy of the nodes.

This work is based on two stages which are:

Stage 1: Conventional technique for Detection

Advanced techniques such as cooperative sensing, authentication-based schemes, machine learning, and cryptographic methods are used to counter PUE attacks and enhance detection and resilience. Cooperative frequency determination further supports identifying and mitigating PUE attacks for secure Cognitive Radio Network (CRN) operations. In this section, we explain the conventional mechanism for detecting PUEA.

The conventional technique for PUEA

In the conventional algorithms of PUEA Detection, the source of the spectrum information is validated as depicted in Figure 1 below. The key aspect of this method is its ability to verify the authenticity of a signal source based on its location. If the calculated distance, determined by two different techniques, matches, the user is considered trustworthy. Conversely, if there is a distance discrepancy, the user is deemed malicious.

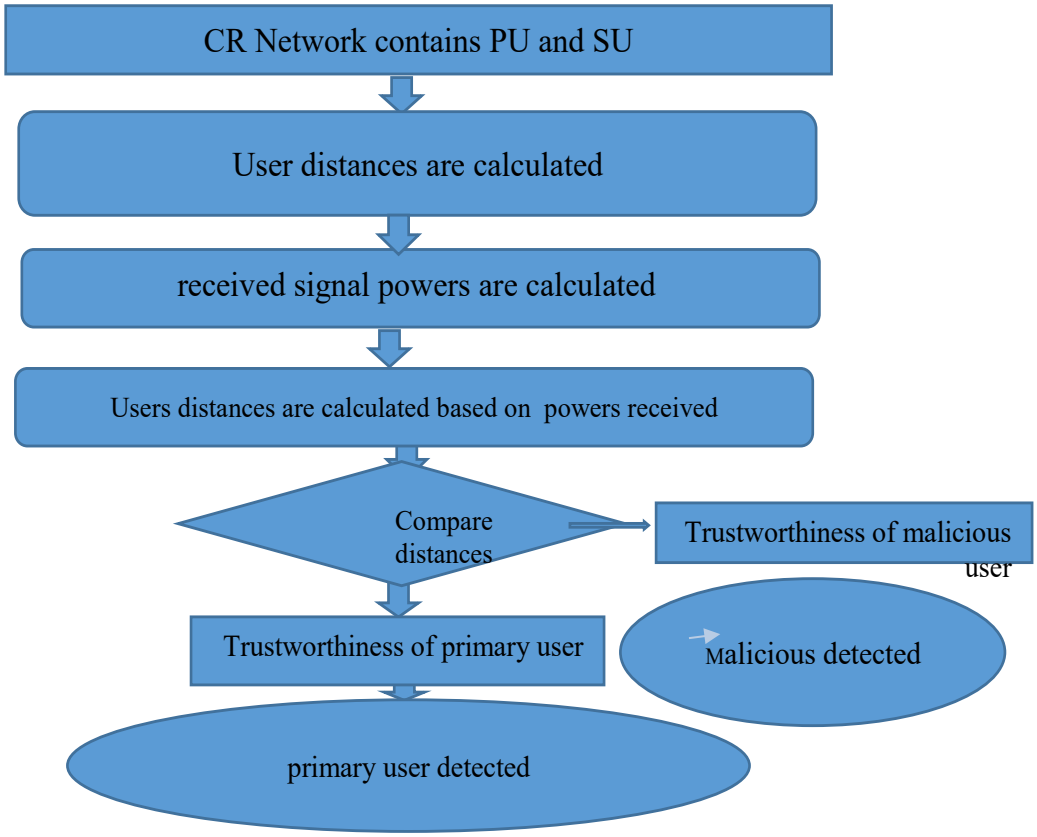


Figure (1). The conventional Technique for PUEA Detection

The cognitive radio (CR) network follows a specific set of steps, with one key condition: if the calculated distances match, the signal source is considered legitimate. If the distances do not align, the transmitter is regarded as unauthorized.

Using users' locations

The nodes distance Y is computed based on their geographical coordinates. For example, if (A, B) are the points of user location and (C, D) are the points of the primary user, a

$$Y= ((A-C)^2+(B-D)^2)^{1/2} \quad * \qquad (1)$$

In this work, it is assumed that all nodes (primary and secondary users) broadcast their location coordinates to be used in the calculation.

Using signal power

The concept of measuring distance based on received signal strength (RSS) or received power is grounded in the assumption that received power is related to both the transmitting power and the distance between the two radio devices. The distance between a secondary user and another device can be estimated by measuring the received signal power and knowing the transmit power level. The received power P_r with a given transmit power P_t is described by:

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \quad * \qquad (2)$$

G_t and Gr = gain of the signal , h_t, h_r = the transmitter and receiver length , L= loss factor It's considered that all variables above in equation 2 are assumed to be 1 except Pr , P_t and d , so P_r is .

$$P_r = \frac{P_t}{d^4} \quad * \tag{3}$$

$$D = \sqrt[4]{\frac{P_t}{P_r}} \quad * \tag{4}$$

While this method provides an estimate, it is not always accurate due to noise and channel impairments and uncertainties in the signal propagation environment. Despite these limitations, many researchers still favor this approach due to its effectiveness.

Received Signals:
P_r is considered to be without noise is calculated by:

$$(P_r = P_t / d^4) * \tag{5}$$

If the noise is considered, then the power p_r is determined by:

$$(P_r = (P_t + \text{noise}) / d^4) * \tag{6}$$

Nodes Authentication
In this method, a malicious user cannot simultaneously mimic the primary user's coordinates and power level. Consider two distances: d1 is calculated from location coordinates, and d2 is calculated from the received power level. The relative trustworthiness Z of the user is calculated as:

$$Z = \text{Minimum of } (d1/d2 \ , d2/d1) * \tag{7}$$

If both distances match, the user is deemed trustworthy; otherwise, the user is considered malicious. Due to noise, the distance based on received power might not be 100% accurate, but both methods should yield similar results statistically. Trustworthy users will have a trust value close to 1, while untrustworthy users will have lower values.

Stage 2: Proposed algorithm based on the Limited Threshold Range LTR of users trust
Unlike traditional wireless networks, ensuring reliable frequency determination in (CRNs) is crucial for practical deployment. Secondary users (SUs) must accurately detect primary users (PUs) across a wide spectrum with minimal wrong acts. Because the nodes use many modulation methods, it is not easy to detect such acts (Unnikrishnan & Veeravalli, 2008). Energy detection is often chosen when secondary users have limited information about the PU signal because it is simple and computationally inexpensive. However, energy detection can be degraded by issues like (SNR) limitations.

Secondary nodes can work together to improve network outcomes. Cooperative frequency determination is strong to significantly improve the primary users detections (Mishra et al., 2006).

Trust Factor and Limited Threshold Range (LTR)
An SU is allocated with a trust value; if these values are high, it indicates a greater likelihood that the user is legitimate. Users with high trust values are allowed to have more control over the fusion center decision. Unlike conventional cooperative sensing approaches, the proposed method uses a Limited Threshold Range (LTR) for user trust values. This approach enhances network security by distinguishing between legitimate and malicious users. When a user's trust value falls outside the

acceptable range, the Fusion Center excludes that user from contributing to the final decision. The Fusion Center stores the trust values and ensures that suspicious users are excluded from the final decision process. In cases where a collision occurs between a PU and an SU, the PU system is compensated, and the exclusion procedure is applied to the SU system (Ganesan & Li, 2007). If a collision happens and all SUs follow the controller's spectrum-access policy, they will share the penalty. However, if a specific SU violates the policy, the penalty will be applied solely to that user.

The design of the LTR algorithm directly improves detection by using only the appropriate data needed to make the correct decision while ignoring suspected data collected from malicious users. The FC design provides data that strongly supports the research hypothesis. The sampling method is generalized and large data samples are conducted to improve the reliability.

Mechanism of the Cooperative Frequency Determination

We describe the scenario of cooperative frequency determination in (CRNs) and discuss the impact of trust weights and majority rule.

Local Frequency Determination

A CRN is assumed to consist of a primary user, n secondary users, and a Fusion Center; as Figure 2 below explains, each CRN node uses energy detection to sense the spectrum. The hypotheses for whether a PU (H_1) or there is no PU (H_0) :

$$\text{If } X_i(t) = N_i(t) \text{ then } H_o, \text{ or if } X_i(t) = S(t) + N_i(t) \text{ then } H_1 * \quad (8)$$

$$x_{Ei} = \sum_{k=0}^{N-1} |x_i(k)|^2 \quad , i = 1,2,...,M \quad * \quad (9)$$

$X_i(t)$= Received signal for the i^{th} user, X_{EI}= Energy detection Statics at the user i, N= added noise, S is the received signal , M= Users number , N=Samples number , $X_i(k)$= Sample K^{th} of the Received Signal at i^{th} user ,

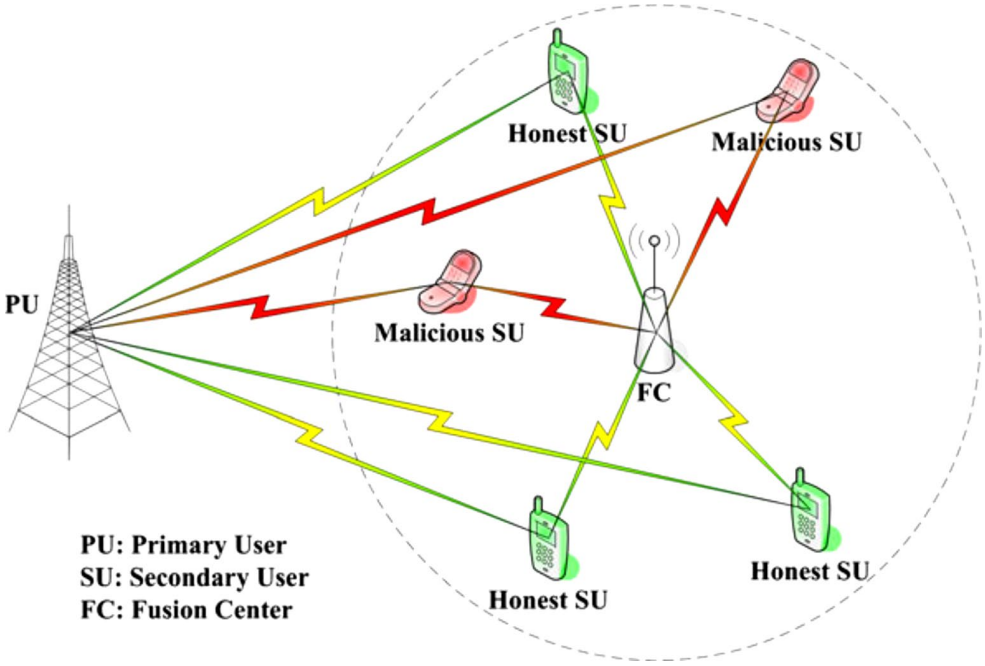


Figure (2). Scenario model of cooperative frequency determination

The decision Ld_i is for the i user. Ld_i =1 primary user is found (H_1), while Ld_i=0 there is no PU (H_0). The energy detection value x_{Ei} and H_0 and H_1, and is expressed as:

$$\begin{cases} x_{Ei} \cong N(\mu_{0i}, \sigma_{0i}^2) & H_0 \\ x_{Ei} \cong N(\mu_{1i}, \sigma_{1i}^2) & H_1 \end{cases}^* \quad (10)$$

σ_{0i}^2 , σ_{1i}^2 represents the variances of H_0 and H_1

LTR Approach

The proposed mechanism enhances frequency determination by utilizing a Limit-Based Trusted Reputation (LTR) method. Unlike traditional majority-based methods that rely solely on the number of users, this model incorporates user reputation scores to make decisions. The key principle is leveraging the input of highly trusted nodes to ensure accuracy and mitigate the influence of malicious or unreliable users.

This approach assigns different weights to nodes based on the assigned score: highly reliable nodes are given greater influence, while unreliable nodes are assigned lower values. Reputation scores, determined by observing behavioral patterns, distinguish between users exceeding a predefined reputation threshold and those deemed reliable, contributing more significantly to the decision-making process. By reducing the impact of unreliable nodes, this scheme improves decision robustness. The algorithm effectively counters the shortcomings of traditional methods, offering a flexible and efficient solution for distributed cooperative frequency determination.

We have added extra security procedures by considering the LTR in addition to the reputation of the user; the central concept of this LTR is that the further away and avoiding being close to the LTR and despite the increase in low-trust users, the more the decision is correct.

LTR Mechanism: The Mechanism of the Proposed LTR Approach is as follows:

λ1, λ2 the lower and upper limit of the range of the Threshold

If User_Reputation R_i<= λ1 and R_i >= λ2

then

$$\left(\text{final\_decision} = \begin{cases} H_1 : \sum_{i=1}^{N} Ld_i R_i > 0 \\ H_0 \quad otherwise \end{cases} \right)$$

When R_i= Node i Reputation, Ldi = Node i decision

RESULTS DISCUSSION

Monte Carlo simulations were conducted using 50,000 samples across varying SNRs to assess the LTR approach. The simulations were run with different numbers of CRN nodes, and Matlab was used to simulate and verify the algorithm. To understand the influence of system parameters on the LTR scheme, the simulations incorporated different penalty factors, with SNR values ranging from -10 to 50 in increments of 5.

(i.e.,-10, -5, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50). As shown in Figure 3 below, the simulation results illustrate the LTR scheme as the number of malicious nodes increases, with varying numbers

of trustworthy users. First, we will examine the outcomes of the conventional majority rule to compare it with the proposed LTR-based method.

Result of the Conventional Mechanism

The mechanisms were simulated with different numbers of reasonable, legitimate, and unreliable nodes to compare both the conventional mechanism rule and the reputation score mechanism. The conventional majority scheme, as shown in Figure 3, operates without assigning reputation values and relies on the number of nodes of the sensing process. The results examine how the number of nodes influences the correct range, taking into account changes in the number of illegitimate nodes.

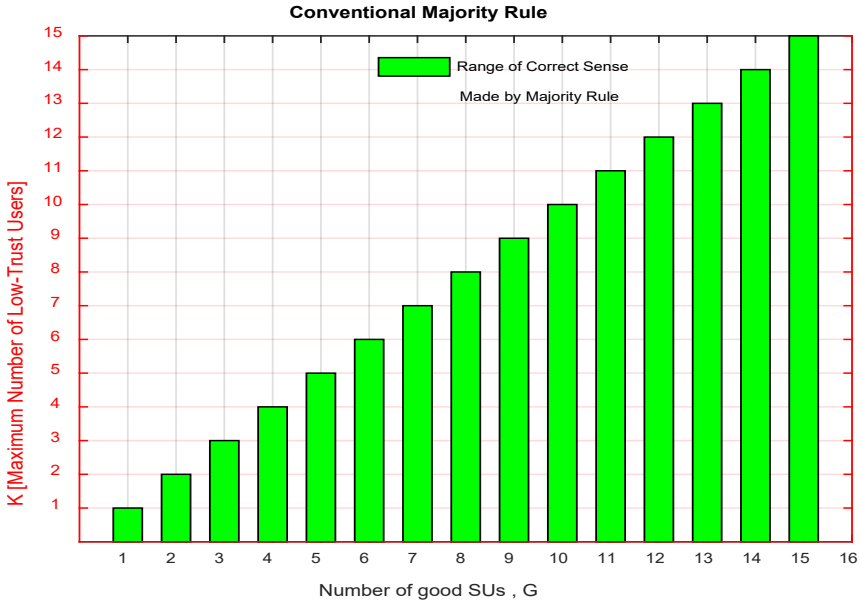


Figure (3). Range of correct sense for different G and K

Figure 3 above is the result of the majority mechanism. For instance, If the number of malicious nodes = 8, then a robust detection is possible only if the bad nodes number <=8. i.e., 50% rule.

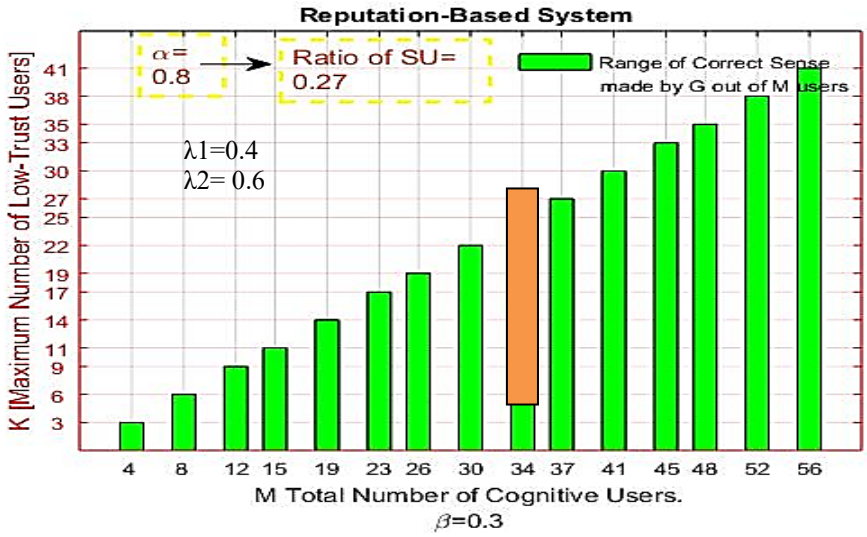
Results of LTR Mechanism

The nodes reputation values and the LTR boundary are used. If the malicious nodes number outcomes the good SU nodes, then a corrected detection is still possible.

First, as shown in Figure 4, the good and malicious nodes reputations are set to 0.8 and 0.3, respectively, and The LTR boundaries are set to $\lambda1=0.4$ $\lambda2= 0.6$. It is noticeable that ten secondary nodes out of 37 nodes are found. This means at least 27% of good users can make a correct decision. The LTR rule is evaluated and simulated by considering the model when the number of nodes M is 34, as explained with the orange bar in Figure 4.

The result in Figure 5 below is obtained when the LTR values are set to ($\lambda1=0.4$ and $\lambda2=0.6$), which means all users whose trust values are in this range are excluded from the decision-making rule.

First, the scheme is evaluated with $\alpha =0.7$ and $\lambda1=0.4$, $\lambda2=0.6$, and it is assumed that the network consists of 34 users with a variant number of low-trust users (malicious users). Figure 5 shows that the correct decision is made when the ratio of low-trust users is up to 0.65, i.e., more than 0.65 of malicious users in the cooperative radio network will lead to a wrong detection.



Figure(4) Reputation System

In comparison with the results obtained by (Letaief & Zhang, 2009), our results outperform theirs in terms of the number of users required to make the correct decision.

Secondly, the scheme is evaluated with α =0.8 and λ1=0.4, λ2=0.6, i.e. the users trust value is changed and set farther from the LTR values. It is noticed that from Figure 5. The correct decision is made even when the ratio of low-trust users is up to 0.71, i.e. increasing the good users trust value makes the network able to tolerate the presence of up to 0.71 of malicious users in the cooperative radio network, more than that ratio of malicious users will also lead to a wrong decision.

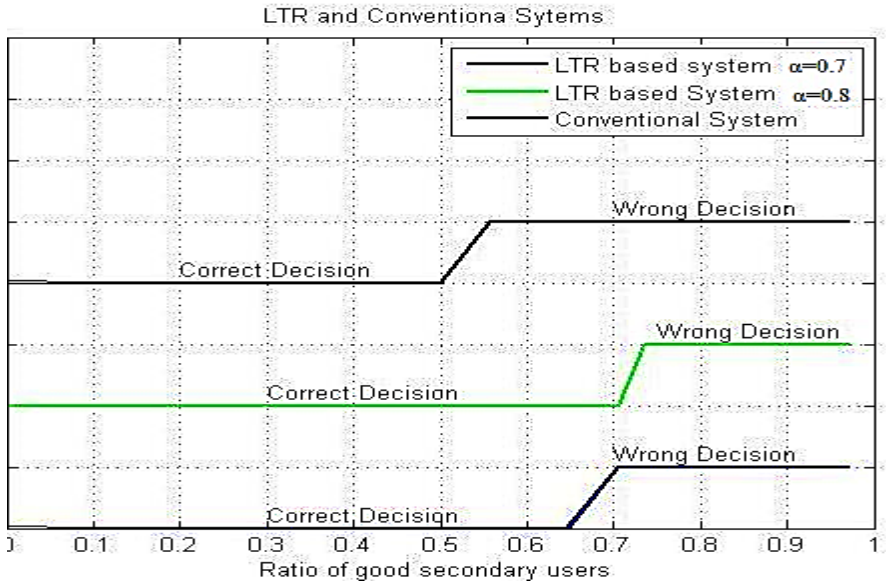


Figure (5). Proposed LTR Scheme

The conventional scheme could only tolerate up to 50% of malicious users. As shown in Figure 5 above i.e., more than 50% of malicious users will lead to a wrong decision according to the conventional scheme.

CONCLUSION

The Limited Threshold Range (LTR)--based cooperative frequency determination approach offers an effective mechanism for the challenges of the limited spectrum. reallocating the spectrum to secondary users without causing interference with primary users. by utilizing cooperative frequency determination, the overall efficiency of spectrum usage can be significantly enhanced. However, secondary users must ensure the reliability and legitimacy of the spectrum occupancy information they rely on. To address this concern, we have proposed schemes incorporating reputation-based mechanisms and penalties to ensure secure access to the spectrum in cognitive radio networks.

In this work, each node independently determines frequency and forwards its local sensing data to a primary central node. The schemes effectively minimize the influence of low-reputation users while enhancing the contribution of high-reputation users.

The LTR scheme improves the performance of cooperative frequency determination, even in networks with varying numbers of trustworthy and unreliable users. The scheme significantly enhances decision accuracy by excluding low-trust users from the decision-making process. Simulation outcomes show that the LTR scheme outperforms the traditional majority-based approach.

Future Research Directions

The proposed scheme can be refined through practical, experimental, and laboratory testing. Future developments could focus on the following directions:

- **Distributed Frequency determination (DSS):** Incorporating DSS to detect primary nodes accurately.
- **Evaluation of RSSI-Based Transmitter Identification using USRP:** To defend against Primary User Emulation Attacks (PUEA) experimentally, we suggest conducting hardware experiments with software-defined radio (SDR). A transmitter identification method based on a Received Signal Strength Indicator (RSSI) at varying frequencies could be used to identify transmitters at different locations. The method can be validated in indoor environments using USRP devices.

Duality of interest: The authors declare that they have no duality of interest associated with this manuscript.

Author contributions: Contribution is equal between authors.

Funding: No specific funding was received for this work.

REFERENCES

Akyildiz, I. F., Lo, B. F., & Balakrishnan, R. (2011). Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical communication, 4*(1), 40-62.

Chen, R., & Park, J.-M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. 2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks,

Digham, F. F., Alouini, M.-S., & Simon, M. K. (2003). On the energy detection of unknown signals over fading channels. IEEE International Conference on Communications, 2003. ICC'03.,

Ganesan, G., & Li, Y. (2007). Cooperative spectrum sensing in cognitive radio, part II: multiuser networks. *IEEE Transactions on wireless communications, 6*(6), 2214-2222.

Ghasemi, A., & Sousa, E. S. (2007). Opportunistic spectrum access in fading channels through collaborative sensing. *J. Commun., 2*(2), 71-82.

Hossain, E., & Bhargava, V. K. (2007). *Cognitive wireless communication networks*. Springer Science & Business Media.

Letaief, K. B., & Zhang, W. (2009). Cooperative communications for cognitive radio networks. *Proceedings of the IEEE, 97*(5), 878-893.

Mishra, S. M., Sahai, A., & Brodersen, R. W. (2006). Cooperative sensing among cognitive radios. 2006 IEEE International conference on communications,

Simon, M. K., & Alouini, M.-S. (2005). Digital Communication over Fading Channels, John Wiley & Sons. *Inc., Publication*.

Unnikrishnan, J., & Veeravalli, V. V. (2008). Cooperative sensing for primary detection in cognitive radio. *IEEE Journal of selected topics in signal processing, 2*(1), 18-27.