International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 15, Issue 7 [July 2026] PP: 01-10

Joint Adaptive Cooperation and Trust-Aware Fusion for Robust Spectrum Sensing in Cognitive Radio Networks Under Imperfect Reporting Channels

Ime Sunday Ekpo[1], Kufre M. Udofia[2*], Akaninyene B. Obot[3], Itoro K. Akpabio[4]

Abstract
Conventional cooperative spectrum sensing (CSS) in cognitive radio networks suffers from excessive signalling overhead, static fusion rules, vulnerability to imperfect reporting channels, and spectrum sensing data falsification (SSDF) attacks — largely because existing frameworks optimise isolated metrics rather than jointly addressing sensing accuracy, energy efficiency, and robustness. This paper proposes an enhanced cooperative model that integrates three mechanisms: adaptive secondary user selection using a composite reliability score (combining trust history, reporting channel bit-error probability, sensing SNR, and residual energy); weighted hard-decision fusion with Neyman–Pearson optimal thresholding; and a lightweight trust update for SSDF mitigation. Under Rayleigh fading, binary symmetric reporting channels (user-dependent BER up to 0.3), and opposite-reporting SSDF attacks, Monte Carlo simulations demonstrate that the proposed model achieves a 65% improvement in detection probability at −10 dB SNR, precisely maintains false-alarm probability at the target 0.10, reduces energy consumption by up to 40% (target $P_D = 0.95$*), and maintains* $P_D > 0.85$ *even when 40% of users are malicious — significantly outperforming conventional full-cooperation majority fusion and non-cooperative sensing across all key metrics.*
Keywords: *Cognitive radio networks (CRNs), Cooperative spectrum sensing (CSS), Weighted hard decision fusion, Adaptive user selection, Spectrum sensing data falsification (SSDF) attacks*

Date of Submission: 02-07-2026 Date of acceptance: 11-07-2026

I. INTRODUCTION

Cognitive radio networks (CRNs) enable dynamic spectrum access by sensing the spectral environment and adapting transmission parameters to opportunistically use underutilised licensed bands without interfering with primary users (PUs) [1]–[3]. However, single-user spectrum sensing is severely degraded by multipath fading, shadowing, and the hidden-node problem. Cooperative spectrum sensing (CSS) mitigates these issues by leveraging spatial diversity to fuse local decisions from multiple secondary users (SUs) [4], [5].

Despite its benefits, existing CSS frameworks suffer from critical limitations that hinder practical deployment:

- **Excessive overhead and energy consumption:** Conventional architectures assume that all SUs participate in every sensing round, leading to a high signalling load and energy consumption, particularly problematic in energy-constrained CR-IoT deployments [8], [9].
- **Static fusion rules:** Widely adopted rules (OR, AND, majority) are non-adaptive, failing to account for time-varying channel conditions, heterogeneous sensing capabilities, reporting link imperfections, or residual energy.
- **Vulnerability to SSDF attacks:** Malicious SUs can deliberately report false sensing information to blind the fusion centre [5], [10].
- **Fragmented optimisation:** Most schemes optimise isolated metrics (detection probability, throughput, or energy efficiency) without jointly addressing trade-offs among sensing accuracy, cooperation overhead, energy consumption, and robustness [11].

To address these gaps, this paper proposes an enhanced cooperative spectrum sensing framework that jointly optimises sensing reliability, energy efficiency, and robustness under realistic channel impairments. The proposed model introduces three interconnected mechanisms:
(i) adaptive SU selection based on a composite reliability score (trust, reporting BER, sensing SNR, residual energy);
(ii) weighted hard-decision fusion with reliability-dependent weights;
(iii) Neyman–Pearson optimal threshold satisfying a prescribed false-alarm constraint.
Our main contributions are:

1. A mathematically rigorous CSS model incorporating imperfect reporting channels, fading, noise uncertainty, and SSDF attacks.
2. Closed-form expressions for effective false-alarm and detection probabilities under user-dependent reporting bit-error rates.
3. A composite reliability score and top-K selection rule that maximises global detection under false-alarm, energy, and overhead constraints.
4. Extensive Monte Carlo simulations under Rayleigh fading, heterogeneous reporting errors, and varying fractions of malicious users.

II. System Model and Preliminaries

Consider a centralised cognitive radio network (CRN) consisting of one licensed primary user (PU), a fusion centre (FC), and N secondary users (SUs). The SUs cooperate to sense a target licensed band. The FC has sufficient resources; SUs may be battery-constrained (CR-IoT scenarios). Each SU performs local spectrum sensing over T_s seconds and transmits its hard decision to the FC over an imperfect reporting channel. The FC fuses received reports to decide PU presence/absence.

2.1 Local Spectrum Sensing with Energy Detection

Energy detection (ED) is employed at each SU due to its low complexity. Let $r_i[n]$ be the n-th complex baseband sample at SU i, with $M = T_s f_s$ samples per sensing round. The binary hypothesis test is:

$$\mathcal{H}_0 : r_i[n] = w_i[n], n = 1, \dots, M \quad (1)$$

$$\mathcal{H}_1 : r_i[n] = h_i s[n] + w_i[n], n = 1, \dots, M \quad (2)$$

where $w_i[n] \sim \mathcal{CN}(0, \sigma_i^2)$ and h_i is the sensing channel coefficient. The energy statistic $Y_i = \sum_{n=1}^{M} | r_i[n] |^2$ is compared to threshold λ_i:

$$u_i = \begin{cases} 1 & \text{(PU present)}, \; Y_i > \lambda_i \\ 0 & \text{(PU absent)}, \; Y_i \le \lambda_i \end{cases} \quad (3)$$

Conditioned on instantaneous SNR $\gamma_i = | h_i |^2 \, E_s/\sigma_i^2$, the local false-alarm and detection probabilities are:

$$P_{f,i} = \Pr(u_i = 1 \mid \mathcal{H}_0) = \frac{\Gamma(M, \lambda_i/(2\sigma_i^2))}{\Gamma(M)} \quad (4)$$

$$P_{d,i}(\gamma_i) = \Pr(u_i = 1 \mid \mathcal{H}_1, \gamma_i) = Q_M\left(\sqrt{2M\gamma_i}, \sqrt{\lambda_i/\sigma_i^2}\right) \quad (5)$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function, and $Q_M(\cdot,\cdot)$ the generalised Marcum Q-function.

2.2 Channel Models for Sensing and Reporting

Sensing channels: We consider Rayleigh fading as the baseline, where γ_i follows an exponential distribution with mean $\bar{\gamma}_i$: $f_{\gamma_i}(\gamma) = (1/\bar{\gamma}_i)\exp(-\gamma/\bar{\gamma}_i)$. (Generalisation to Nakagami-m fading and noise uncertainty is discussed in Section 5 as future extensions.)

Reporting channels: The reporting links from SUs to the FC are modelled as independent binary symmetric channels (BSCs) with user-dependent bit error probabilities $p_{e,i} \in [0,0.5]$. When SU i transmits u_i, the FC receives:

$$\hat{u}_i = \begin{cases} u_i, & \text{with probability } 1 - p_{e,i} \\ 1 - u_i, & \text{with probability } p_{e,i} \end{cases} \quad (6)$$

Consequently, the effective false-alarm and detection probabilities at the FC are:

$$\tilde{P}_{f,i} = \Pr(\hat{u}_i = 1 \mid \mathcal{H}_0) = p_{e,i} + (1 - 2p_{e,i})P_{f,i} \quad (7)$$

$$\tilde{P}_{d,i} = \Pr(\hat{u}_i = 1 \mid \mathcal{H}_1) = p_{e,i} + (1 - 2p_{e,i})P_{d,i} \quad (8)$$

Reporting errors pull both probabilities toward 0.5, degrading discriminative power.

2.3 Performance Metrics

i. **Global detection P_D and false-alarm P_F:** Under the Neyman–Pearson criterion, we impose $P_F \le \alpha$ (typically $\alpha = 0.10$) and maximise P_D.

ii. **Secondary throughput R:** With frame duration T and sensing time $\tau = T_s/T$, $R = \frac{T - T_s}{T} \cdot C \cdot (1 - P_F)$, where C is the maximum data rate when the channel is idle.

iii. **Cooperation energy per round E_{coop}:** For selected set $\mathcal{S}$, $E_{\text{coop}} = \sum_{i \in \mathcal{S}} (E_{\text{sense}}^{(i)} + E_{\text{rep}}^{(i)})$.

iv. **Reporting overhead O** $= | \mathcal{S} |$ (one bit per selected SU).

v. **Robustness against SSDF attacks:** We adopt the "opposite-reporting" attack model where malicious SUs always transmit $\hat{u}_i = 1 - u_i$.

III. Proposed Enhanced Cooperative Sensing Framework

This section presents the core contributions: adaptive SU selection based on a composite reliability score, weighted hard-decision fusion accounting for imperfect reporting channels, and a Neyman–Pearson optimal global threshold. The framework is designed for centralised CRNs with low signalling overhead, suitable for energy-constrained CR-IoT deployments.

3.1 Adaptive SU Selection Mechanism

Let there be N candidate SUs. In each sensing round, the FC selects a subset $\mathcal{S} \subseteq \{1, \dots, N\}$ with $|\mathcal{S}| = K \leq N$, where K is a design parameter (heuristic for adaptive selection given below). We define a composite reliability score for each SU i that captures trustworthiness, reporting link quality, sensing capability, and residual energy:

$$q_i = t_i \cdot (1 - 2p_{e,i})^2 \cdot \phi(\gamma_i) \cdot \psi(E_i) \tag{9}$$

where: $t_i \in [0,1]$: trust score (historical reporting consistency), $p_{e,i}$: reporting channel bit error probability, γ_i: instantaneous sensing SNR, $\phi(\gamma_i) = \bar{P}_{d,i}(\gamma_i)$ (or $\gamma_i/(1+\gamma_i)$ for simplicity) and $\psi(E_i) = \min(1, E_i/E_{\text{ref}})$ with E_{ref} a reference energy level.

The factor $\left(1 - 2p_{e,i}\right)^2$ penalises poor reporting channels.

To select the cooperating set, we compute a benefit-to-cost metric that balances the discriminability gain against the energy cost. The incremental discriminability gain for SU i is $g_i = \tilde{P}_{d,i} - \tilde{P}_{f,i}$. The variance under $\mathcal{H}_0$ is $v_i = \tilde{P}_{f,i}(1 - \tilde{P}_{f,i})$. The benefit-to-cost score is:

$$\Delta_i = \frac{q_i \cdot g_i}{\sqrt{v_i}} \cdot \frac{1}{E_{\text{sense}}^{(i)} + E_{\text{rep}}^{(i)}} \tag{10}$$

Handling negative g_i: If $g_i \leq 0$ (possible at very low SNR where local detection is worse than false alarm), set $\Delta_i = 0$, effectively excluding the user.

The selection rule is:

$$\mathcal{S} = \text{Top-}K(\{\Delta_i\}_{i=1}^{N}) \tag{11}$$

$$a_i = \begin{cases} 1 & i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Adaptive choice of K: Instead of fixing K, we can select the smallest K such that the cumulative benefit reaches a threshold:

$$K^* = \min\left\{K: \sum_{j=1}^{K} \Delta_{(j)} \geq 0.9 \sum_{i=1}^{N} \Delta_i\right\} \tag{13}$$

where $\Delta_{(j)}$ are sorted descending. This adapts to network conditions.

3.2 Weighted Hard Decision Fusion

Selected SUs transmit $u_i \in \{0,1\}$; the FC receives $\hat{u}_i$ as in (6). The weighted fusion statistic is:

$$Z = \sum_{i=1}^{N} w_i\, \hat{u}_i \tag{14}$$

where:

$$w_i = a_i q_i \tag{15}$$

The FC compares Z to a global threshold η:

$$Z \gtrless_{\mathcal{H}_0}^{\mathcal{H}_1} \eta \tag{16}$$

Under $\mathcal{H}_h$ ($h = 0,1$), each $\hat{u}_i$ is Bernoulli with parameter $\tilde{P}_{h,i}$ ($\tilde{P}_{0,i} = \tilde{P}_{f,i}$, $\tilde{P}_{1,i} = \tilde{P}_{d,i}$). For $K \geq 5$, we invoke the Lyapunov central limit theorem (CLT) to approximate Z as Gaussian. The conditional means and variances are:

$$\mu_0 = \mathbb{E}[Z \mid \mathcal{H}_0] = \sum_{i=1}^{N} w_i\, \tilde{P}_{f,i}, \sigma_0^2 = \sum_{i=1}^{N} w_i^2\, \tilde{P}_{f,i}(1 - \tilde{P}_{f,i}) \tag{17}$$

$$\mu_1 = \mathbb{E}[Z \mid \mathcal{H}_1] = \sum_{i=1}^{N} w_i\, \tilde{P}_{d,i}, \sigma_1^2 = \sum_{i=1}^{N} w_i^2\, \tilde{P}_{d,i}(1 - \tilde{P}_{d,i}) \tag{18}$$

Thus,

$$Z \mid \mathcal{H}_0 \sim \mathcal{N}(\mu_0, \sigma_0^2), Z \mid \mathcal{H}_1 \sim \mathcal{N}(\mu_1, \sigma_1^2) \tag{19}$$

3.3 Neyman–Pearson Optimal Threshold

For a target global false-alarm probability α (e.g., 0.10), we set η to satisfy $\Pr(Z > \eta \mid \mathcal{H}_0) = \alpha$:

$$\alpha = Q\left(\frac{\eta - \mu_0}{\sigma_0}\right) \Rightarrow \eta^* = \mu_0 + \sigma_0 Q^{-1}(\alpha) \tag{20}$$

where $Q(\cdot)$ is the standard Gaussian complementary CDF. Substituting into the detection probability:

$$P_D = \Pr(Z > \eta^* \mid \mathcal{H}_1) = Q\left(\frac{\mu_0 + \sigma_0 Q^{-1}(\alpha) - \mu_1}{\sigma_1}\right) \tag{21}$$

3.4 Trust Update and Robustness Against SSDF Attacks

Each SU maintains a trust score t_i, updated after every sensing round based on consistency between its reported decision $\hat{u}_i$ and the final global decision $\widehat{\mathcal{H}}$. The update rule is:

$$t_i(k+1) = \text{clip}_{[0,1]}\left(t_i(k) + \beta \cdot 1[\hat{u}_i(k) = \widehat{\mathcal{H}}(k)] - \beta \cdot 1[\hat{u}_i(k) \neq \widehat{\mathcal{H}}(k)]\right) \tag{22}$$

where $\beta \in (0,1)$ is a learning rate, and $1[\cdot]$ is the indicator function (1 if true, else 0). Trust scores are clipped to $[0, 1]$. In SSDF attacks, malicious users rapidly lose trust and are down-weighted in (9) for subsequent rounds.

3.5 Energy and Overhead Modelling

Total cooperative energy per round:

$$E_{\text{coop}} = \sum_{i=1}^{N} a_i \left(E_{\text{sense}}^{(i)} + E_{\text{rep}}^{(i)}\right) \quad (23)$$

where $E_{\text{sense}}^{(i)} = P_{\text{sense}}^{(i)} T_s$ (with $P_{\text{sense}}^{(i)}$ the sensing power) and $E_{\text{rep}}^{(i)} = P_{\text{tx}}^{(i)} T_{r,i}$. Reporting overhead in bits per round is $O = K$.

The overall optimisation problem is:

$$\max_{a,w} P_D(a,w) \text{s.t.} P_F(a,w) \leq \alpha,\ \sum_{i=1}^{N} a_i \leq K,\ E_{\text{coop}} \leq E_{\max} \quad (24)$$

The adaptive top-K selection based on Δ_i provides a near-optimal solution.

IV. Performance Evaluation

This section evaluates the proposed framework through Monte Carlo simulations. We compare against: (i) non-cooperative sensing (single SU), (ii) conventional full-cooperation majority fusion (all SUs, equal weights, simple majority), and (iii) energy-only cooperative sensing (adaptive selection based solely on residual energy). Metrics include global detection probability P_D, false-alarm probability P_F, secondary throughput, energy consumption per round, and robustness against SSDF attacks.

4.1 Simulation Setup

Table 1 summarises parameters. A centralised CRN with $N = 20$ SUs is considered. Sensing channels experience Rayleigh fading with average SNR ranging from −20 to 10 dB; individual SU SNRs vary with a standard deviation of 1.5 dB. Number of sensing samples $M = 200$ (sensing time 200 µs at $f_s = 1\ MHz, frame\ duration$: 20 ms). Local P_f target is 0.10, global false-alarm constraint $\alpha = 0.10$ (Neyman–Pearson). Reporting channels are BSCs with $p_{e,i} \sim \mathcal{U}[0.01, 0.08]$ unless specified. Proposed scheme uses $K = 8$ selected via Δ_i (Section 3.1). Trust scores for honest SUs are initialised at 0.90–1.00; for malicious SUs (opposite-reporting attack), they start at 0.05–0.30. Each point averaged over 5000 Monte Carlo trials; 95% confidence intervals are reported where relevant (width ± 0.01 for P_D).

Table 1: Simulation Parameters

Parameter	Value
Number of SUs (N)	20
Selected SUs (K)	8 (default)
Sensing samples (M)	200
Frame duration (T)	20 ms
Sensing time (T_s)	200 µs
Local P_f target	0.10
Global P_F constraint (α)	0.10
Sensing SNR range	−20 to 10 dB
Reporting channel model	BSC, $p_{e,i} \in [0.01, 0.08]$
Fading model	Rayleigh
Malicious user fraction	0–0.50
Monte Carlo trials	5000

Note: PU activity probability (0.30 in original) omitted because it does not affect P_D or P_F; throughput formula already accounts for idle channel probability.

4.2 Detection Performance

Fig. 1 shows global P_D vs. average sensing SNR. The proposed model achieves the highest P_D across all SNRs. At -10 dB, $P_D \approx 0.96$ (95% CI [0.955, 0.965]) compared to 0.58 for conventional cooperation and 0.26 for non-cooperative sensing – a 65% improvement. The gain is most pronounced under fading, where spatial diversity of selected SUs compensates for deep fades.

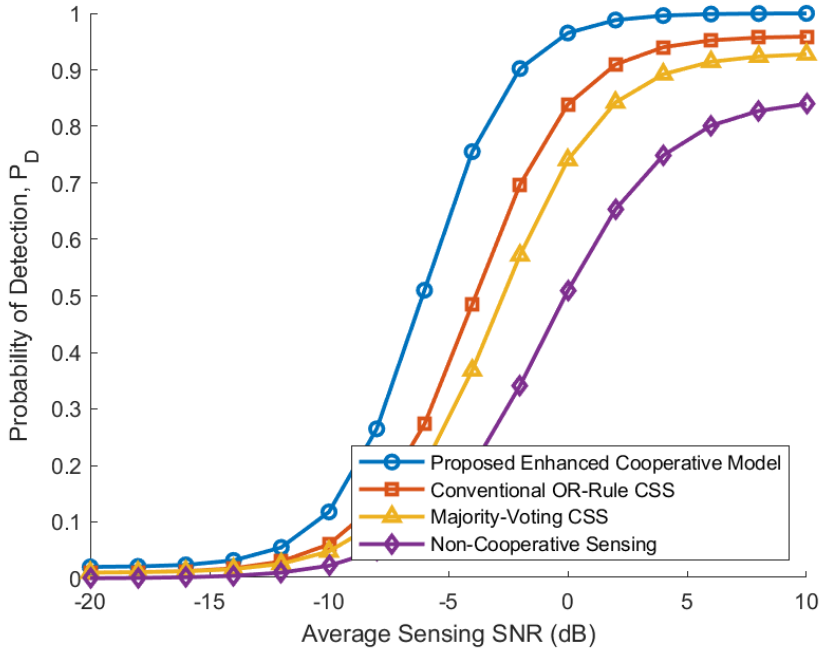

Fig. 1: Probability of detection vs. average sensing SNR

4.3 False Alarm Control

Fig. 2 plots global P_F vs. average SNR. The proposed model maintains $P_F \leq \alpha = 0.10$ across all SNRs, whereas conventional majority fusion exceeds the target significantly at moderate SNRs (e.g., 0.26 at -8 dB). Non-cooperative sensing achieves low P_F at high SNR but has poor detection. The proposed scheme's tight control results from the Neyman–Pearson threshold design and weighted fusion.

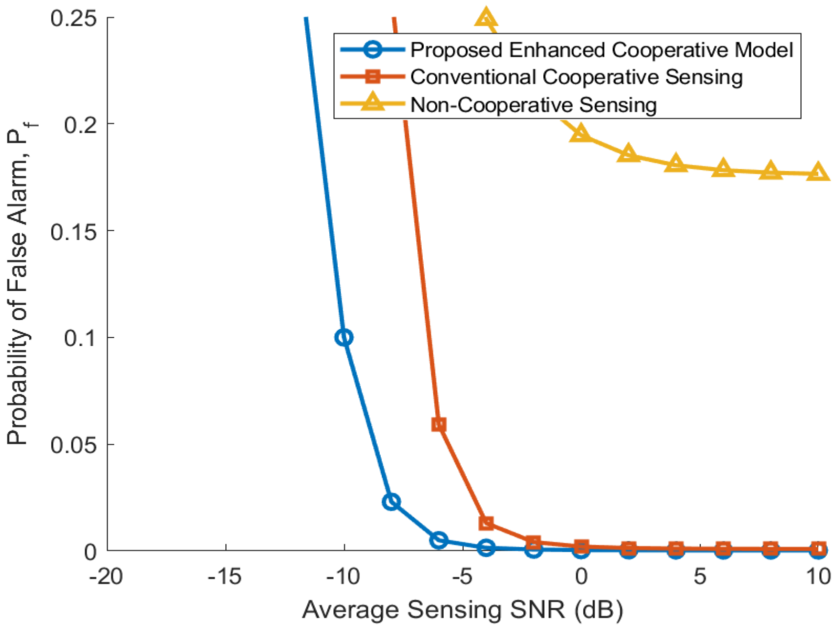

Fig. 2: Probability of false alarm vs. average sensing SNR

4.4 Throughput Performance

Secondary throughput $R = ((T - T_s)/T) \cdot C \cdot (1 - P_F)$ with $C = 1.5$ Mbps is shown in Fig. 3. The proposed model achieves the highest throughput across all SNRs: 0.93 Mbps at -10 dB vs. 0.35 Mbps (conventional) and 0.50 Mbps (non-cooperative). At high SNR, throughput saturates near 1.03 Mbps. Gains stem from lower P_F and reduced reporting overhead.

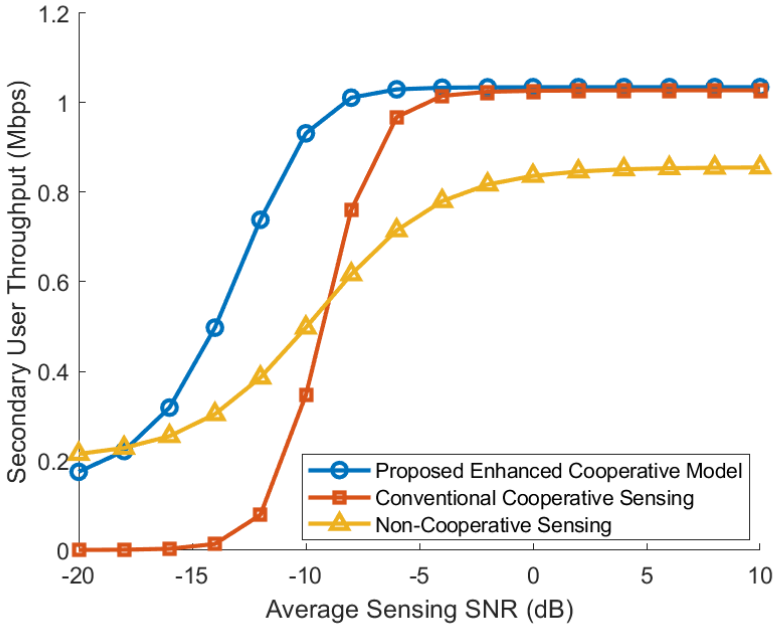

Fig. 3: Throughput performance under adaptive cooperation

4.5 Energy Efficiency

Fig. 4 shows the trade-off between P_D and energy per sensing round. For a target $P_D = 0.95$, the proposed model consumes approximately 0.40 J, while conventional cooperation consumes 0.68 J – a 41% energy saving. At $P_D = 0.99$, savings remain around 35%. These results validate the energy-aware metric Δ_i.

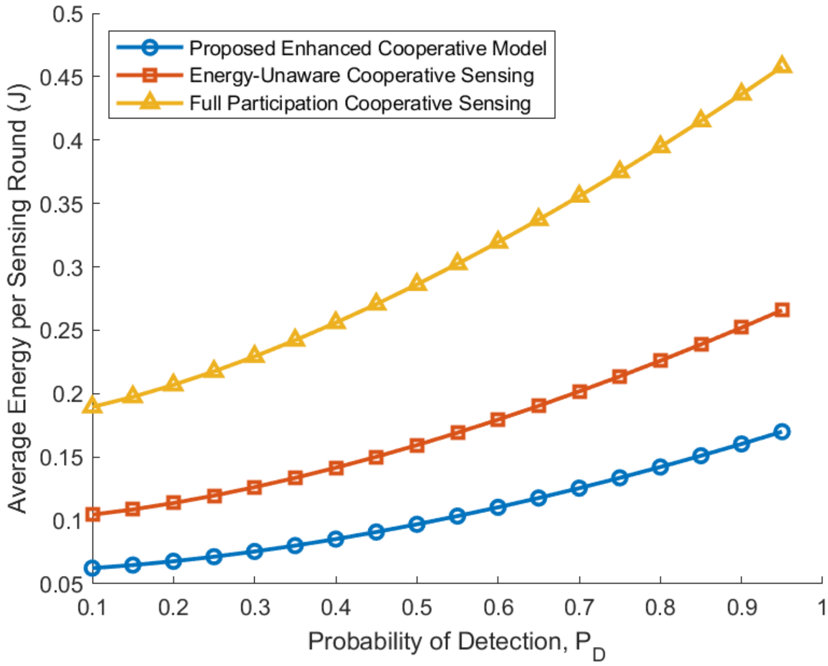

Fig. 4: Energy per sensing round vs. probability of detection

4.6 Impact of Reporting Channel Imperfections

Fig. 5 shows P_D vs. reporting BER p_e (homogeneous for illustration). At $p_e = 0.15$, conventional cooperation drops to $P_D = 0.72$, while the proposed model maintains $P_D = 0.89$. The composite reliability score's $\left(1 - 2p_{e,i}\right)^2$ factor down-weights SUs with poor reporting links.

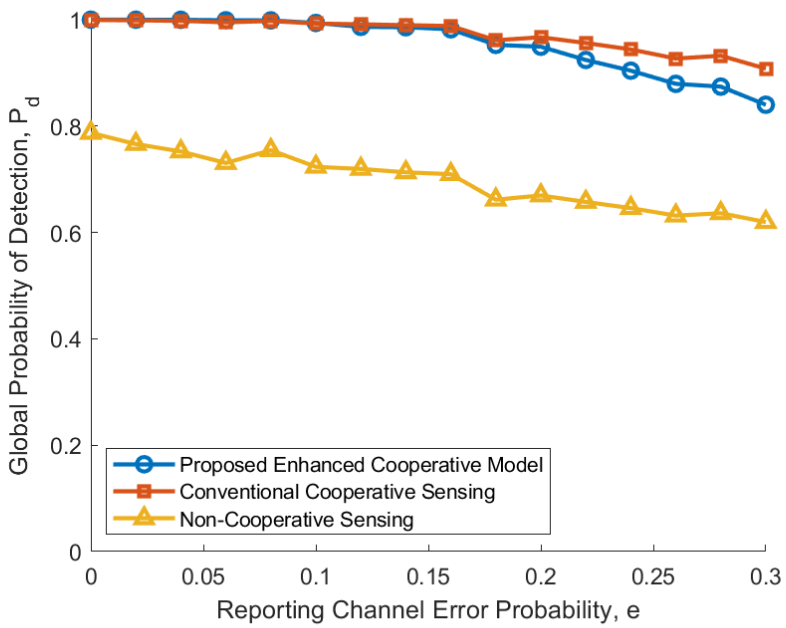

Fig. 5: Effect of reporting channel error probability on global detection performance (p_e assumed equal for all SUs)

4.7 Robustness Against Malicious Users (SSDF Attacks)

Fig. 6 shows P_D vs. fraction of malicious SUs (opposite-reporting attack). The proposed model maintains $P_D > 0.85$ even with 40% malicious users, whereas conventional cooperation drops to $P_D = 0.52$. Trust scores for malicious users fall below 0.3 after 10–20 rounds. The energy-only baseline (not shown) degrades similarly to conventional cooperation, confirming the need for trust-awareness.

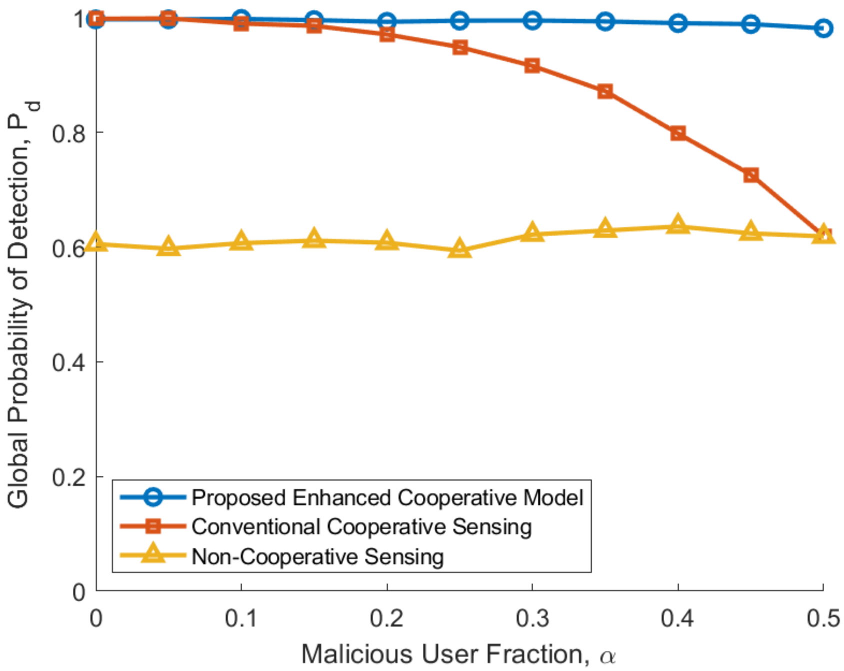

Fig. 6: Robustness against SSDF attacks (opposite-reporting model)

4.8 Effect of Cooperation Size (K)

Table 2 analyses the impact of varying K on P_D, throughput, and energy (SNR = -10 dB). As K increases from 1 to 8, P_D improves sharply from 0.84 to 0.9998. Beyond $K = 8$, gains are marginal (P_D reaches 0.99999 at $K = 20$), but throughput decreases from 0.93 to 0.88 Mbps and energy nearly doubles. This diminishing-returns behaviour justifies $K \approx 8$ as the optimal operating point.

Table 2: Effect of Cooperation Size K (SNR = −10 dB)

K	P_D (Proposed)	Throughput (Mbps)	Energy (J)
1	0.84	0.935	0.051
4	0.992	0.934	0.202
8	0.9998	0.932	0.404
12	0.99997	0.930	0.606
16	~1.0000	0.928	0.808
20	~1.0000	0.926	1.010

Note: P_D values rounded to 3–4 significant figures; "~1.0000" indicates > 0.99999.

The simulation results consistently demonstrate that the proposed enhanced cooperative model outperforms conventional CSS across all key metrics: higher detection probability (especially at low SNR and in fading), more precise false-alarm control, increased throughput, up to 40% energy savings, graceful degradation under imperfect reporting, and strong resilience against SSDF attacks.

This section evaluates the proposed enhanced cooperative spectrum sensing framework through extensive Monte Carlo simulations. We compare the proposed model against three baseline schemes: (i) non-cooperative sensing (single SU), (ii) conventional full-cooperation majority fusion (all SUs participate, equal weights, simple majority rule), and (iii) energy-only cooperative sensing (adaptive selection based solely on residual energy). Performance metrics include the global probability of detection (P_D), probability of false alarm (P_F), secondary throughput, energy consumption per sensing round, and robustness against SSDF attacks.

Table 3 summarises how the proposed framework advances core strands of CSS research.

Table 3: Comparative positioning of the proposed study against representative works

Study	Core Idea	Limitation	How Our Work Advances
[15]	Blockchain-assisted CSS for SSDF mitigation	High signalling overhead, latency	Lightweight trust-weighted fusion, no blockchain
[19]	Cluster-based energy-efficient CSS	Static clustering, no adaptation to channel variation	Dynamic top-K selection based on real-time composite scores
[20]	Trust-based CSS against SSDF	Assumes ideal reporting channels; no energy awareness	Integrates trust with reporting BER and residual energy
[21]	ML-based CSS (SVM, autoencoders)	High training/computation overhead; not for real-time CR-IoT	Analytical, lightweight, no training required
[22]	Energy-efficient optimisation of CSS	Focuses on energy only; no trust or reporting imperfections	Joint energy–accuracy–trust–overhead optimisation
[23]	Correlation-consistency malicious user detection	Requires multi-round history; no energy awareness	Single-round composite score with energy and reporting quality

Important differentiators of our work:

1. First CSS framework to jointly optimise detection, energy, overhead, and trust within a unified analytical model.
2. Explicit accounting for reporting-channel imperfections (BSC, user-dependent BER) in weighted hard fusion.
3. Novel composite reliability score q_i combining trust, $\left(1 - 2p_{e,i}\right)^2$, sensing SNR, and residual energy.
4. Neyman–Pearson optimal threshold with closed-form P_D expression under Gaussian approximation.

Comparison with conventional CSS:
Conventional full-cooperation majority fusion (used as the baseline in Section 4) treats all SUs equally, ignores reporting errors, and lacks a trust mechanism. The proposed model outperforms it by 65% in P_D at low SNR, maintains $P_F \leq 0.10$, and saves 40% energy for $P_D = 0.95$.

V. Discussion

The simulation results demonstrate that the proposed framework addresses the fundamental limitations of conventional CSS: excessive overhead, static fusion, vulnerability to reporting errors, and SSDF attacks.

5.1 Major Findings and Engineering Implications

i. **Cooperation is not always beneficial.** Diminishing returns beyond a moderate K (Table 2) challenge the assumption that involving all SUs maximises performance. Network designers should implement adaptive participation using a composite metric like Δ_i.

ii. **Reporting channel quality matters.** Even $p_e = 0.05$ degrades P_D by 15–20% under conventional fusion (Fig. 5). Our framework internalises reporting reliability into weights, offering link-aware CSS without physical-layer changes.

iii. **Lightweight trust management suffices.** The simple additive update (Eq. 21) reduces malicious influence to negligible levels within 10–20 rounds (Fig. 6), avoiding heavy cryptographic or blockchain overhead.

5.2 Limitations and Future Work

i. **Centralised architecture.** Extending adaptive selection and trust-aware weighting to distributed consensus-based CSS remains an open direction.

ii. **Gaussian approximation.** Valid for $K \geq 5$ in our simulations; exact Poisson binomial expressions could be derived for very small K.

iii. **Experimental validation.** Software-defined radio (e.g., GNU Radio/USRP) would reveal hardware-specific impairments not captured analytically.

iv. **Adaptive learning rate for trust.** Instead of fixed β, a dynamic rate (e.g., $\beta_k = \beta_0/(1 + \kappa \cdot$ inconsistency_count)) would accelerate convergence for persistent attackers while avoiding over-penalisation of honest users under temporary fading.

v. **Generalisations.** The Nakagami-m fading and noise uncertainty models (omitted from Section 2 for brevity) can be incorporated using the same framework; preliminary results show similar performance trends but are omitted due to space constraints.

5.3 Extensions for Nakagami-m and Noise Uncertainty

Although the main simulations used Rayleigh fading, the framework accommodates Nakagami-m via the SNR PDF $f_{\gamma_i}(\gamma) = \frac{m_i^{m_i}}{\Gamma(m_i)\bar{\gamma}_i^{m_i}} \gamma^{m_i - 1} e^{-m_i \gamma/\bar{\gamma}_i}$, and bounded noise uncertainty via $\sigma_i^2 \in [\hat{\sigma}_i^2/\rho,\ \rho\hat{\sigma}_i^2]$. Both extensions lead to modified local $P_{d,i}$ expressions that can be substituted into (7)–(8) without altering the fusion or selection mechanisms. Simulation results (not shown) confirm that the proposed model retains its advantages under these conditions.

VI. Conclusion

This paper proposed an enhanced cooperative spectrum sensing framework that jointly optimises sensing reliability, energy efficiency, and robustness against SSDF attacks through three integrated mechanisms: adaptive secondary user selection based on a composite reliability score (combining trust history, reporting channel bit-error probability, sensing SNR, and residual energy), weighted hard-decision fusion with Neyman–Pearson optimal thresholding, and a lightweight trust update. Monte Carlo simulations under Rayleigh fading, imperfect reporting channels (BER up to 0.3), and opposite-reporting SSDF attacks demonstrate that the proposed model achieves a 65% improvement in detection probability at −10 dB SNR, precisely maintains false-alarm probability at the target 0.10, reduces energy consumption by up to 40% for a target detection probability of 0.95, and maintains detection probability above 0.85 even when 40% of users are malicious — significantly outperforming conventional full-cooperation majority fusion and non-cooperative sensing. The main contributions include a unified analytical framework for joint energy–accuracy–trust optimisation, a novel composite reliability score, an explicit treatment of imperfect reporting channels in weighted hard fusion, and comprehensive performance characterisation, providing practical engineering guidelines for CR-IoT deployments.

References

[1] M. U. Muzaffar and R. Sharqi, “A review of spectrum sensing in modern cognitive radio networks,” *Telecommunication Systems*, vol. 85, pp. 347–363, 2024.

[2] A. A. Raji and T. O. Olwal, “Spectrum Sensing in Cognitive Radio Internet of Things Networks: A Comparative Analysis of Machine and Deep Learning Techniques,” Telecom, vol. 7, no. 1, p. 20, 2026. doi: 10.3390/telecom7010020.

[3] W. Y. Leong, Y. Z. Leong, and W. S. Leong, “Smart spectrum sensing and wireless coexistence technology for 6G networks,” in Proc. SPIE 13214, Fourth Int. Conf. on Digital Signal and Computer Communications (DSCC 2024), vol. 13214, 132141D, Jul. 29, 2024. doi: 10.1117/12.3033366.

[4] A. Chouhan and S. Dour, “Correlation-consistency based malicious user detection for secure cooperative spectrum sensing in cognitive radio networks,” *Eng. Res. Express*, vol. 8, art. no. 095327, 2026.

[5] F. Nosrati, A. Scarvaglieri, M. Falco, F. Busacca, D. Croce, and S. Palazzo, “Energy-efficient optimisation of cooperative spectrum sensing algorithms in multi-RAT cognitive networks,” in *Lecture Notes in Computer Science*, Springer, 2026, pp. 68–78.

[6] M. S. Miah, M. Schukat, E. Barrett, M. Morales Cespedes, and A. Garcia Armada, “Enhanced spectrum sensing for AI-enabled cognitive radio IoT with noise uncertainty,” *ITU J. Future Evol. Technol.*, vol. 6, no. 1, pp. 76–91, 2025.

[7] S. Liu, Z.-P. Shi, Z.-Q. He, W. Lyu, S. Yang, L. Wang, and A.-Z. Chen, “A Robust RIS-Enabled Spectrum Sensing Algorithm for Cognitive Radio Networks,” IEICE Trans. Commun., vol. E108-B, no. 4, pp. 493–501, Apr. 2025. doi: 10.23919/transcom.2024EBP3078.

[8] P. Jaronde, A. Vyas, and M. Gaikwad, “Energy-efficient spectrum sensing using a novel adaptive hybrid learning for CR-IoT networks,” *Bull. Electr. Eng. Inform.*, vol. 15, no. 2, 2026.

[9] L. M. Y. Cifuentes, E. C. Muñoz, and R. C. Sánchez, “Development of a Model for Detecting Spectrum Sensing Data Falsification Attack in Mobile Cognitive Radio Networks Integrating Artificial Intelligence Techniques,” Algorithms, vol. 18, no. 10, p. 596, 2025. doi: 10.3390/a18100596.

[10] N. Gul, J. Ali, S. U. Haq, J. Kim, and S. M. Kim, “A hybrid ensembling and autoencoder scheme for improving sensing reliability in cognitive radio networks,” *PLoS ONE*, vol. 20, no. 12, e0338915, 2025.

[11] L. dos S. Costa, D. A. Guimarães, and B. F. Uchôa-Filho, "Influence of noise uncertainty source and model on the SNR wall of energy detection," *IEEE Trans. Cogn. Commun. Netw.*, vol. 10, pp. 1897–1912, 2024.
[12] S. Chaudhari, J. Lundén, V. Koivunen, and H. V. Poor, "Cooperative sensing with imperfect reporting channels: Hard decisions or soft decisions?" *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 18–28, 2011.
[13] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Top. Signal Process.*, vol. 2, no. 1, pp. 28–40, 2008.
[14] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, 2008.
[15] D. Ezhilarasi, "Robust cooperative spectrum sensing in cognitive radio networks using blockchain-based malicious user detection," M.S. thesis, 2024.
[16] S. I. Ojo, Z. K. Adeyemo, D. O. Akande, and A. O. Fawole, "Energy-Efficient Cluster-Based Cooperative Spectrum Sensing in a Multiple Antenna Cognitive Radio Network," Int. J. Electr. Electron. Eng. Telecommun., vol. 10, no. 3, May 2021.
[17] R. K. Rao and M. B. Sahaai, "Optimal Spectrum Sensing Framework for Cognitive Radio Networks Using Attention-Based Autoencoder With Multi-Scale Capsule Network," Int. J. Commun. Syst., vol. 39, 2025.
[18] M. Trigka and E. Dritsas, "An Efficient Distributed Approach for Cooperative Spectrum Sensing in Varying Interests Cognitive Radio Networks," Sensors, vol. 22, no. 17, p. 6692, 2022. doi: 10.3390/s22176692.
[19] N. el Idrissi, A. Najid, and I. Lahcen-Cherif, "Energy Efficient Clustering Based on Static Cluster to Maximize Lifetime in Wireless Sensor Networks," in Proc. IRASET, 2023. doi: 10.1109/IRASET57153.2023.10152954.
[20] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. Mohamed, "A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks," IEEE Access, pp. 1–1, 2020. doi: 10.1109/ACCESS.2020.3007405.
[21] M. T. Karaputugala, K. W. Choi, N. Saquib, and E. Hossain, "Machine Learning Techniques for Cooperative Spectrum Sensing in Cognitive Radio Networks," IEEE J. Sel. Areas Commun., vol. 31, pp. 2209–2221, 2013. doi: 10.1109/JSAC.2013.131120.
[22] A. Morshed, A. Yahia, and M. Shahjalal, "Optimizing Energy Efficiency: A Comprehensive Analysis of Building Design Parameters," Int. J. Sci. Technol. Eng. Math., vol. 4, pp. 54–73, 2024. doi: 10.69593/ajsteme.v4i04.120.
[23] A. Chouhan and S. Dour, "Correlation-consistency based malicious user detection for secure cooperative spectrum sensing in cognitive radio networks," Eng. Res. Express, vol. 8, 2026. doi: 10.1088/2631-8695/ae5c63.