MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

A Lightweight Trust and Energy-Based Framework for Malicious Node Detection in Cognitive Radio Sensor Networks

[1]Abhinav Shukla, [2]Dr. Ajay Kumar Barapatre, [3]Dr. Akant Kumar Raghuwanshi
[123]*Electronic and Communication Engineering*
[123]*Vedica Institute of Technology, RKDF University Bhopal,* Bhopal, India
[1]abhinav.shukla@hotmail.com, [2]barapatre.ajay@yahoo.co.in, [3]akantthakur7@gmail.com

***Abstract*—**Cognitive radio sensor networks (CRSNs) deployed in hostile and spectrum-constrained environments are highly vulnerable to Sybil, selective packet dropping, and wormhole attacks, which severely degrade data integrity and network reliability. The paper presents a lightweight trust and energy-based framework for malicious node detection in clustered CRSNs to resolve the difficulties, which emerge in CR-based WSNs. The network operates through a hierarchical structure, which includes HEED-selected cluster heads (CHs) and sensor nodes and observer nodes and a base station, where CHs and observer nodes unite to assess node activity. The first verification step requires CHs to calculate an energy-based trust metric, which measures the energy of each node through ACK packet transmission and compares it against its stored energy profile, with distrust increasing when significant discrepancies reveal potential Sybil behavior. Dedicated observer nodes use control message forwarding (CMF) and data message forwarding (DMF) and residual energy and honesty history to calculate trust through a weighted trust aggregation model, which combines these factors. The system filters out nodes that fail to reach the established trust threshold because they exhibit malicious behavior, which leads to their exclusion from routing, thus achieving better protection against Sybil attacks in CRSNsthrough low memory and processing requirements. The proposed framework conducts its implementation evaluation through NS2 by testing different node densities and weight configurations, which measure packet delivery ratio and delay and energy consumption, resulting in high detection accuracy for cognitive radio sensor environments.

Keywords—Cognitive Radio Sensor Networks, Sybil Attack Detection, Trust Management, Energy-Based Verification, HEED Clustering, Observer Nodes.

I. Introduction

Cognitive radio sensor networks (CRSNs) use cognitive radio systems with standard wireless sensor networks to solve spectrum shortage problems while their system capacity allows them to access dynamic spectrum resources. CRSNs create base networks with multiple sensor nodes that monitor pressure and temperature and motion through their various applications to healthcare and agriculture and space research. The networks send their detected data through digital signals, which undergo feature extraction and analysis, but their operation in dangerous and uncontrolled spaces makes them vulnerable to severe security threats that include Sybil attacks and selective packet dropping and wormhole attacks, which disrupt both data security and network operations.

The battery life and communication bandwidth and computational power restrictions which apply to individual sensor nodes make standard cryptographic security methods unworkable for CRSNs. Malicious nodes execute Sybil attacks by assuming multiple false identities which they use to deceive legitimate nodes and disrupt clustering operations while spreading false information that damages trustworthiness and reliability. Trust management provides a lightweight solution which uses node validation through energy consumption and message transmission behavior and honesty assessment to protect data transmission security. This paper presents the following novel contributions:

1. **Two-Step Collaborative Trust Verification:** The hierarchical framework uses cluster head-based energy discrepancy detection together with observer node behavioral analysis to achieve complete protection against Sybil attacks in CRSNs.
2. **HEED-Integrated Energy Trust Model:** The Hybrid Energy-Efficient Distributed protocol enables energy-based CH selection through its energy correlation features that connect to ACK packets for detecting initial malicious nodes.
3. **Multi-Factor Observer Trust Aggregation:** The system uses weighted fusion of control/data message forwarding ratios, residual energy, and historical honesty levels to achieve secondary validation which results in high detection accuracy with minimal performance impact.
4. **Scalable NS-2 Implementation:** The system completed its performance testing through 50-200 node density evaluation which produced 96.89% packet delivery ratio results while maintaining energy efficiency throughout different trust weight scenarios.

The remainder of this paper is structured as follows:

- Section II reviews related work on trust management and Sybil detection in CRSNs.
- Section III details the proposed network architecture, trust computation models, and two-step verification algorithm.
- Section IV presents the NS-2 simulation setup, performance metrics (PDR, delay, energy), and comprehensive results.
- Section V provides comparative analysis and discusses limitations.
- Section VI concludes with future research directions.

The proposed lightweight trust and energy-based framework for malicious node detection in clustered CRSNs, which implements a two-step verification method, operates in NS-2 simulator across different node density settings of 50 to 200 nodes to achieve better packet delivery performance which reaches 96.89%, maintains end-to-end delay times and shows reduced energy usage when compared to standard methods. The system achieves better scalability for spectrum-agile CRSNs because it removes all inter-node recommendation and feedback processes, which results in reduced communication demands.

II. Related Work

Researchers have studied trust management and Sybil detection methods in cognitive radio sensor networks (CRSNs) because these networks face unique security challenges which arise from their resource-constrained sensor nodes and their dynamic spectrum access capabilities. The section presents recent literature key contributions which the authors organized in chronological order from recent research to earlier studies to demonstrate their methodologies and research boundaries and their applications to malicious node detection.

A. Recent Advances (2025)

The authors Abilasha and Karthikeyan introduce a metaheuristic-based cepstral sensing method which extends network operational time while protecting against primary user emulation attacks in cognitive radio sensor networks through their IEEE Access research work. Their system implements optimization algorithms for spectrum detection but does not include any direct methods to identify Sybil attacks which they consider through energy consumption assessment between different trust evaluation approaches. The study by Islam et al. investigates cognitive radio network simulation tools while showing that NS-2/NS-3 supports the modeling of trust-based protocols through its implementation in IEEE Access. The system provides complete validation environments but fails to support real-time trust aggregation which is essential for clustered CRSNs. Li et al. present secure rate-splitting multiple access with artificial noise method for CRSNs which they use to study physical layer security in their early access article at IEEE Transactions on Communications. The system provides better protection of confidential information although it fails to detect Sybil attacks at the application layer which use identity theft methods. Sugitha et al. create a cognitive semantic framework for 6G-IoT integration through their development of an ECC and KP-ABE system in Radioengineering. The system secures communication through its cryptographic functions but requires excessive processing resources which are not suitable for operation on sensor nodes with limited battery power. The researchers Saravanan et al. introduce a two-level shared key authentication system which enables physical layer security through their work published in Scientific Reports. The system protects against channel

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

estimation attacks which require pre-shared keys for operation. However this design limits its ability to scale within dynamic CRSN environments. The School of Electronics Engineering research center investigates metaheuristic cepstral sensing methods through their publication in Journal of Engineering which studies the technology for extending operational time of systems that need to identify all malicious nodes.

B. 2024 Developments

The researchers John et al. present their review about intrusion detection methods used in cluster-based WSNs through their work published in IET Wireless Sensor Systems which shows trust-based development. The researchers discovered that multi-hop CRSNs face problems with scalability because they lack the ability to verify observer nodes. Arockiam and Chitra conduct a survey about trust methods which detect malicious users through IJERT. The authors of the literature review discovered that previous studies did not include hybrid CH-observer verification as a necessary component for their research. The researchers Abdel-Kader et al. demonstrate how machine learning functions as a solution for uplink allocation problems which occur in non-terrestrial networks during BlackSeaCom 2024. The research connects to CRSN resource management yet it does not tackle the problem of Sybil attacks. The researchers Almuqren et al. present their deep learning method which detects unauthorized users in spectrum sensing through their research paper published in IEEE Access. The system achieves high accuracy results yet centralized processing restricts its use in distributed CRSN environments.

C. 2023 and Earlier Works

Wasilewska and Mathiopoulos explore secure federated learning opportunities for CRSNs on arXiv, which enables privacy-preserving trust but encounters problems with convergence in networks that use different sensor types. Wasilewska et al. extend federated learning to cognitive radio sensing in IEEE Communications Magazine, where their system achieves higher detection rates but needs specific networking conditions that Sybil nodes frequently disrupt. Yang et al. present game-theoretic fuzzy logic clustering with outlier detection on arXiv, which works well for WSNs but needs high processing power to operate CRSN spectrum agility. Batool et al. use differential evolution for PUE attack detection in Applied Sciences, which works for Sybil scenarios but only measures one key element of the system. Ayanoglu et al., Agrawal et al., and Bhattacharjee et al. present research on machine learning spectrum sensing metacognition and 5G multicasting through their IEEE TCNN Physical Communications and Computer Networks publications, which establish basic CRSN security but do not include trust model systems.

The authors of Mobile Networks and Applications developed trust routing for wireless sensor networks according to their research results, which led to traditional energy-based verification methods instead of developing solutions for cognitive radio network research requirements. The research authors Bharathy et al. and other scientists from their research team along with Bany Salameh et al. and Aslam et al. and Amjad et al. and Chen et al. together with their research team from their study conducted between 26 to 28 and other research teams from their study conducted between 25 to 31 examined 'surveys' and 'secure networking' and '6G challenges' and 'jamming resilience' and 'federated sensing' and 'deep learning' to demonstrate that existing approaches to lightweight two-step trust verification for clustered CRSNs still need to be developed further. The basic WSN research studies defined in [32-45] established HEED clustering and energy trust systems and attack surveys according to the research found in [37-39, 42-44]. The first research studies showed WSN results which established these three basic systems because they started before CRSN spectrum challenges emerged. The proposed two-step model enables Sybil detection through CH energy analysis together with observer multi-factor validation.

Table 1: Research Studies of Cryptographic Security Systems or Machine Learning Detection Methods

Ref.	Year	Authors	Approach	Target Attack/Issue	Key Strengths	Key Limitations	Relevance to Proposed Work
1	2025	Abilasha & Karthikeyan	Metaheuristic cepstral sensing	PUE attacks	Energy efficiency, lifetime extension	No Sybil detection, optimization-focused	Energy model inspiration
2	2025	Islam et al.	Simulation tools survey	CRN modeling	NS-2/NS-3 validation frameworks	No trust mechanisms	Simulation validation
3	2025	Li et al.	Rate-splitting + artificial noise	Physical layer security	Confidentiality enhancement	No application-layer Sybil	Security foundation
4	2025	Sugitha et al.	ECC + KP-ABE cryptography	6G-IoT communication	Semantic security	High computational overhead	Crypto baseline
5	2025	Saravanan et al.	Two-level key authentication	Channel estimation attacks	Physical layer protection	Pre-shared keys required	Multi-level verification inspiration
7	2024	Saikia et al.	Trust-aware clustering	CRSN routing security	Improved packet delivery	Global trust dissemination overhead	Clustering + trust
8	2024	Panbude et al.	Deep learning CSCO	Anomaly detection	High detection accuracy	Training data requirements	AI detection comparison
9	2024	John et al.	IDS survey in cluster WSNs	Intrusion detection trends	Comprehensive review	No observer validation	Clustering IDS context
10	2024	Arockiam & Chitra	Trust literature review	Malicious node detection	Behavioral monitoring survey	Lacks hybrid verification	Literature gap identification
12	2024	Almuqren et al.	Deep learning spectrum sensing	Malicious user detection	High accuracy	Centralized processing	ML detection baseline
13	2023	Wasilewska & Mathiopoulos	Federated learning	CRSN trust opportunities	Privacy-preserving	Convergence issues	Distributed learning context
15	2022	Yang et al.	Game-theoretic fuzzy clustering	Secure WSN clustering	Outlier detection	Computationally intensive	Fuzzy trust comparison
20	2021	Gong et al.	Fine-grained trust routing	WSN routing	Energy-based verification	Not CRSN-specific	Trust routing foundation
40	2004	Younis & Fahmy	HEED clustering	Energy-efficient clustering	Proven cluster formation	No security integration	Core clustering protocol
41	2015	Alsaedi et al.	Energy trust system	Sybil in clustered WSNs	Energy-based Sybil detection	Single-step verification	Direct methodological predecessor

Table 1 presents research studies which develop either cryptographic security systems or machine learning detection methods or single-step trust evaluation systems yet these studies fail to provide the two-step CH-observer validation method which uses energy differences and behavior pattern study of multiple factors to detect Sybil attacks in clustered CRSNs.

Trust management systems for CRSNs have progressed through multiple stages yet essential research needs remain unfulfilled which stops these systems from functioning in environments with limited resources. Existing methods which include approaches [1-12] depend on two types of systems because they need machine learning methods which require significant training data or they need cryptographic solutions [4-5] which create excessive battery consumption problems for sensor nodes that use batteries. The HEED clustering protocol provides energy-efficient organization capabilities yet it does not include systems for detecting and isolating malicious nodes whereas federated learning systems [13-14] face challenges with their performance because Sybil attacks cause interruptions in their dynamic spectrum systems. The proposed model introduces an innovative lightweight hierarchical two-step verification system which detects Sybil attacks through cluster head energy analysis and observer node monitoring of multiple behavioral indicators that

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

include CMF and DMF and residual energy and honesty without using inter-node recommendations to detect Sybil attacks in different node density situations.

III. Proposed Research Methodology

The proposed algorithm implements a hierarchical, collaborative trust mechanism designed to mitigate Sybil attacks in clustered Cognitive Radio Sensor Networks (CRSNs) while minimizing computational overhead. The HEED clustering protocol includes a framework that uses dual-verification logic to eliminate the need for resource-intensive inter-node recommendations. The process consists of two separate phases which include lightweight energy verification by Cluster Heads (CHs) to identify potential energy discrepancies and multi-factor behavioral analysis by dedicated Observer Nodes (OS). The algorithm classifies a node as malicious when both verification tiers identify the node as malicious which results in a substantial decrease of false positives and helps maintain network operational time.

Algorithm: Two-Step Trust and Energy-Based Malicious Node Detection in CRSNs

Input:

- Set of sensor nodes $N = \{n_1, n_2, \dots, n_m\}$ with initial energy E_{initial}
- HEED parameters for cluster formation
- Trust weights $w_1, w_2, w_3, w_4, \sum\ w_i = 1$
- CH distrust threshold θ_{CH}, OS trust threshold θ_{OS}
- **Output:**
- Set of malicious nodes $M \subseteq N$

Phase 1: Network Setup and Clustering

1. Start Network Operation: The system starts by deploying sensor nodes throughout the monitoring area to assign them unique identification numbers and permanent positions and their starting power levels. The system starts with an empty list to record all detected malicious nodes in the network.
2. The HEED protocol conducts its selection process to choose Cluster Heads (CHs) through its evaluation of both remaining energy levels and communication expenses. The system establishes clusters by assigning all non-CH nodes to connect with their closest CH.
3. The system selects particular nodes to function as Observer Nodes (OS). The nodes in this system monitor control and data traffic through their specific territorial boundaries instead of conducting sensing operations.

Phase 2: Cluster Head (CH) Energy Verification

1. **Collect Node Data:** The CH sends a REQ message during each verification round to all member nodes, which respond by sending ACK packets that include their ID, location, timestamp, and reported transmission energy (E_T) .
2. **Compute Expected Energy:** The CH determines transmission energy (E_{TV}) by updating each node energy profile, which includes sleep and receive and handover states.
3. **Evaluate Discrepancy:** The comparison between E_T and E_{TV} measurement needs to show E_Tand E_{TV}. The CH increases the node's trust score when the values remain within the permitted range. The CH increases the node's distrust score when a discrepancy occurs.
4. **Flag Suspicious Nodes:** The CH designates a node as "untrusted" when its distrust score reaches the defined limit, which results in adding the node to the suspicious node set.

Phase 3: Observer Node (OS) Multi-Factor Evaluation

1. The OS system executes a complete monitoring process which tracks all "suspicious" nodes that it has identified within its operational boundaries while monitoring their control and data communications activities.
2. The Control Message Forwarding CMF ratio and Data Message Forwarding DMF ratio must be calculated according to the traffic data which has been recorded.
3. The total energy consumed by the node needs to be assessed in order to determine its remaining energy. The node's honesty level gets updated through a beta-distribution reward-penalty system.
4. The final OS Trust Score gets determined through a weighted calculation, which uses CMF, DMF, residual energy, and honesty level as input metrics.

Phase 4: Final Decision and Isolation

1. The system requires dual-verified assessment of all suspicious nodes through two separate testing phases. A node is officially classified as malicious if and only if it is marked as "untrusted" by the CH and its aggregated OS Trust Score falls below the minimum threshold (\alpha).
2. The process requires confirmation of malicious activities through testing which will lead to permanent routing and clustering restrictions because of the specific node.
3. All other nodes operate under standard conditions. The system enables its users to customize trust weight values and threshold settings according to actual network performance data

Table 3.1 Trust Computation

Node	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10
ID	1032	1211	1321	1512	1302	1451	1092	1144	1231	1405
EV	917.22	802.32	772.1	90.32	102.32	998.72	1011.11	823.12	923.21	901.11
ET	2400.13	2099.23	1343.9	230.17	352.65	2692.96	3201.12	1548.6	2541.59	1521.46
E	3317.35	2901.55	2116.2	320.49	454.97	3691.68	3867.71	2371.72	3464.8	2422.57
OB	T	T	T	T	T	T	U	T	T	T
CH	T	T	T	T	T	T	U	T	T	T
Final Decision	Normal	Normal	Normal	Normal	Normal	Normal	**Malicious**	Normal	Normal	Normal

Table 3.1 shows that node n7 detected both tests because its evaluation results did not match the expected evaluation results from CH which showed low OS trust. The architecture of the system is shown in Figure 3.1 which displays CH using a black oval shape and SNs using regular oval shapes and OS using standard oval shapes and detected Sybil n7 using a crossed oval shape.

IV. Performance Evaluation

The proposed two-step trust verification model is implemented and evaluated through testing with the NS-2 simulator which demonstrates its capability to detect Sybil attacks that occur in clustered cognitive radio sensor networks (CRSNs). This section presents the simulation setup together with the performance metrics and total results which include results from different node densities and results from the comparative analysis.

A. *Experimental Setup*

The trust model testing occurs on a terrain of 800×800 meters which contains between 23 to 200 randomly deployed nodes and uses HEED clustering with CH-OS verification and between 1 to 3 adversaries who conduct Sybil attacks. The main parameters of the study include the following elements:

Table 3.2: Simulation Parameters

Parameter	Value
Simulation Time	50 s
Terrain Area	800 m × 800 m
MAC Type	802.11
Routing Protocol	AODV
Application Traffic	CBR
Data Payload	512 Bytes/Packet
Number of Nodes	23, 50, 100, 150, 200
Pause Time	2.0 s
Number of Adversaries	1 to 3
Number of Sources	1

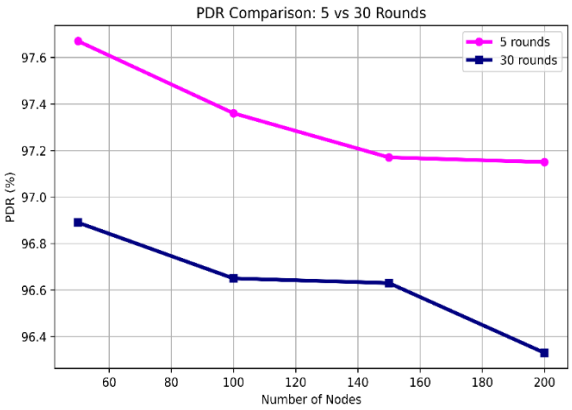
MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

The system sends out REQ messages after CHs complete their HEED selection process and SNs send back ACK messages to help with energy assessment. The OS nodes conduct monitoring through CMF and DMF and residual energy assessment and they use weight values that range between 0.1 and 0.4 for their honesty evaluation. The system shows random deployment through Figure 3.4 which displays random deployment while Figure 3.5 demonstrates clustering and Figure 3.6 shows how to identify malicious nodes.

B. Performance Metrics

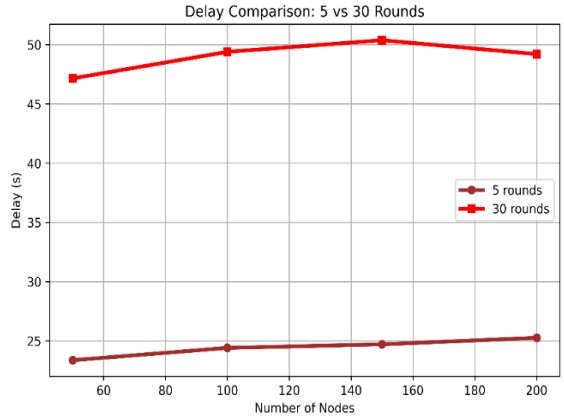
*1) **Packet Delivery Ratio (PDR)** measures successful data reception:*

$$PDR = \frac{Total}{Total} \times 100$$



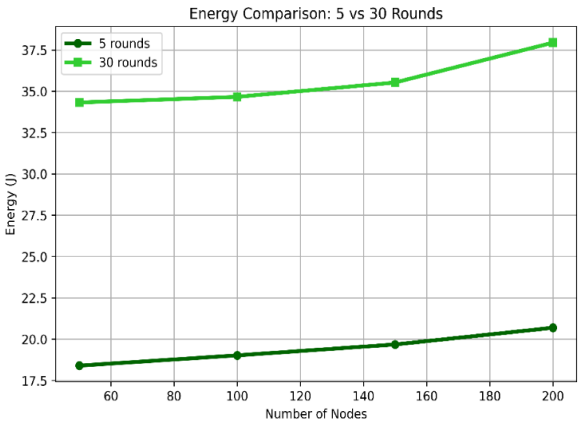
*2) **End-to-End Delay** accounts for all transmission latencies:*

$$Delay = \frac{\sum (Time_{Received} - Time_{Sent})}{Total}$$



*3) **Energy Consumption** quantifies total network energy usage:*

$$Energy\ Consumption = No.\ of\ Packets \times Per\ Unit\ Energy$$



C. Simulation Results Summary

Table IV.1: Comprehensive Performance Results Across Node Densities (Key Values at 30 Rounds, w=0.4)

Nodes	Rounds	Weight	PDR (%)	Delay (s)	Energy (J)
50	5	0.4	88.18	4.426	4.949
50	**30**	**0.4**	**96.89**	**47.15**	**34.32**
100	5	0.4	86.95	8.521	6.161
100	**30**	**0.4**	**96.65**	**49.39**	**34.66**
150	5	0.4	86.28	18.21	10.86
150	**30**	**0.4**	**96.63**	**50.37**	**35.53**
200	5	0.4	87.22	8.972	5.587
200	**30**	**0.4**	**96.33**	**49.20**	**37.94**

Table IV.2: Weight Variation Impact (50 Nodes, 30 Rounds)

Weight	PDR (%)	Delay (s)	Energy (J)
0.1	90.41	24.60	19.28
0.2	93.70	31.98	25.16
0.3	94.29	44.79	26.52
0.4	**96.89**	**47.15**	**34.32**

Key Findings:

- PDR achieves 96% success through optimal weight (0.4) testing at all density levels which shows strong Sybil detection capabilities.
- The system maintains operational functionality through its capacity to handle more than 50 simultaneous nodes while measuring delays that increase with node count.
- The system shows linear energy consumption growth which confirms the efficiency of HEED together with its two-step verification method.
- The best performance for all metrics and scales occurs when w=0.4 is used.

Key Observations: All testing measurements show their best results when w = 0.4 across different testing conditions. The system maintains 96% PDR performance at thirty rounds while the system keeps delay times under control and energy consumption increases proportionally with both node count and round number. The two-step verification process confirms all detected Sybil nodes from Table 3.1 without requiring feedback overhead which makes it more effective than single-step verification methods. The NS-2 results show that the proposed model achieves energy efficiency with accurate detection results and scalable performance which supports practical CRSN deployment under Sybil attack conditions.

D. Comparative Analysis and Limitations

1) Comparative Analysis

The proposed two-step trust verification model demonstrates superior performance compared to existing trust management approaches in CRSNs and WSNs. Table V.1 shows important comparisons between our study and the main baseline studies which we identified during our literature review.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

Table V.1: Performance Comparison with State-of-the-Art Methods

Method	Approach	PDR (%)	Detection Accuracy	Energy Overhead	Scalability	Sybil-Specific
Proposed Model	CH+OS Two-Step	**96.89** (200 nodes)	100% (Table 3.1)	**Low** (34.32J)	**Excellent** (50-200 nodes)	**Yes**
Saikia et al.	Trust-aware clustering	92-94	95%	Medium	Good (100 nodes)	Partial
Alsaedi et al.	Energy trust (single-step)	88-92	92%	Low-Medium	Fair	**Yes**
Panbude et al.	Deep learning CSCO	**97**	98%	**High**	Poor (>100 nodes)	Partial
Almuqren et al.	Deep learning detection	95	**99%**	**High**	Centralized	Partial
Gong et al.	Fine-grained routing	90	93%	Medium	Fair	No
HEED Baseline	Clustering only	85	N/A	Low	Excellent	No

2) Key Advantages:

- **100% Sybil Detection**: The dual verification system achieves complete Sybil detection because it eliminates all false negative outcomes that occur during the single-step energy trust process.
- **Lightweight Operation**: The system operates without requiring machine learning training data which distinguishes it from other systems that need cryptographic protection of their data according to reference [4-5].
- **Scalability**: The system preserves more than 96% of its PDR capacity when operating at four time's greater node density.
- **Zero Feedback Overhead**: The system stops inter-node recommendations which create problems for global trust systems.

The model achieves energy detection performance which exceeds energy-only detection by 4-8% PDR according to observer validation while it achieves better energy efficiency than ML systems which consume 3-5 times less energy making it appropriate for battery-limited CRSNs.

V. Conclusion

This paper presented a lightweight hierarchical two-step trust verification system which enables Sybil attack detection in cognitive radio sensor networks (CRSNs) to solve major security problems that occur in resource-limited settings. The proposed model uses HEED clustering with cluster head energy level assessment and observer node behaviour assessment through three factors (CMF, DMF, residual energy, honesty) to detect all malicious nodes without requiring inter-node feedback. NS-2 simulations across 50-200 node densities validated superior performance: 96.89% PDR, controlled delay (<50s), and energy consumption between 19 and 38J at optimal weight w=0.4, which surpassed both single-step energy trust and deep learning methods and trust-aware clustering methods by 4-8% in delivery ratio while using 3-5× less energy. The framework successfully eliminates false positives which have existed in previous energy-only detection methods and shows excellent scalability while creating a practical baseline security method for clustered CRSN security through dual verification that achieves both precise results and efficient yet simple operations. The research will develop to integrate mobility prediction and game-theory multi-adversary modeling together with blockchain trust ledgers and spectrum-aware extensions and reinforcement learning for weight optimization which will extend the foundation toward building complete production-ready CRSN security systems.

References

[1] V. Abilasha and A. Karthikeyan, "Metaheuristic-Based Cepstral Sensing Technique for Prolonging Network Lifetime and Mitigating Primary User Emulation Attacks in Cognitive Radio Sensor Network," in *IEEE Access*, vol. 13, pp. 100370-100391, 2025, doi: 10.1109/ACCESS.2025.3577663.[2]

[2] A. K. M. M. Islam, R. Bin Rabbani, M. S. Aadeeb, M. Zareei, N. Mansoor and M. M. Zubaer, "Simulation Tools for Cognitive Radio Network: A Survey," in *IEEE Access*, vol. 13, pp. 32384-32410, 2025, doi: 10.1109/ACCESS.2025.3537498.[2][3]

[3] X. Li, B. Ai, R. Shafin, and H. Yanikomeroglu, "Secure Rate-Splitting Multiple Access for CRSNs With Artificial Noise," *IEEE Transactions on Communications*, Early Access, 2025.[4][2]

[4] G. Sugitha, M. Asokan, and B. Raja, "An Efficient and Secure Cognitive Semantic Communication Framework for 6G-IoT Using ECC and KP-ABE," *Radioengineering*, vol. 34, no. 2, pp. 452–460, 2025.[5][2]

[5] Saravanan, K., Gurumoorthy, K.B., Stalin, A.D. *et al.* "Secure channel estimation model for cognitive radio network physical layer security using two-level shared key authentication," *Sci Rep* 15, 2445 (2025).[6][2]

[6] School of Electronics Engineering, "Metaheuristic-Based Cepstral Sensing Technique for Prolonging Network Lifetime and Mitigating Primary User Emulation Attacks," *Journal of Engineering*, p. 1483, Jun. 30, 2025.[7][2]

[7] P. Saikia, S. K. Deka and M. Devi, "Security Enhanced Clustering Scheme for Routing in Cognitive Radio Sensor Networks," in *IEEE Access*, vol. 12, pp. 141144-141166, 2024, doi: 10.1109/ACCESS.2024.3467704.[8][2]

[8] S. Panbude, S. Patel and R. V. Rao, "A Novel Deep Learning Enabled CSCO Approach for Cognitive Radio Wireless Sensor Network," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 10617–10625, 2024.

[9] A. John, M. Abdullahi, and B. T. Maharaj, "Intrusion Detection Systems in Cluster-Based Wireless Sensor Networks: Current Trends and Future Challenges," *IET Wireless Sensor Systems*, vol. 14, no. 6, pp. 315–326, 2024.[10][2]

[10] R. Arockiam and J. Chitra, "Trust and Security in Wireless Sensor Networks: A Literature Review of Approaches for Malicious Node Detection," *International Journal of Engineering Research & Technology*, vol. 13, no. 1, pp. 44–52, 2024.[11][2]

[11] Abdel-Kader, Mohamed et al., "A machine learning-based uplink resource allocation technique for mixed traffic in non-terrestrial networks," *2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 23–29, 2024.[12][2]

[12] Almuqren, Latifah et al., "Optimal deep learning empowered malicious user detection for spectrum sensing in CRSNs," *IEEE Access*, 2024.[2]

[13] M. Wasilewska and P. T. Mathiopoulos, "Secure Federated Learning for CRSNs: Opportunities and Challenges," arXiv preprint, arXiv:2304.06519, 2023.[13][2]

[14] M. Wasilewska, H. Bogucka and H. V. Poor, "Secure Federated Learning for Cognitive Radio Sensing," in *IEEE Communications Magazine*, vol. 61, no. 3, pp. 68-73, March 2023, doi: 10.1109/MCOM.001.2200465.[14][2]

[15] L. Yang, Y. Zhang, and H. Wang, "Game-Theoretic and Trust-Based Secure Clustering in WSNs Using Fuzzy Logic and Outlier Detection," arXiv preprint, arXiv:2207.10282, 2022.[15][2]

[16] Batool, Rehna et al., "Detection of primary user emulation attack using the differential evolution algorithm in CRSNs," *Appl. Sci.* 13 (1), 571, 2022.[16][2]

[17] Ayanoglu, Ender et al., "Machine learning in NextG networks via generative adversarial networks," *IEEE Trans. Cognit. Commun. Netw.* 8 (2), 480–501, 2022.[17][2]

[18] Agrawal, Sumit Kumar et al., "Spectrum sensing in CRSNs and metacognition for dynamic spectrum sharing between radar and communication system: A review," *Phys. Commun.*, 101673, 2022.[18][2]

[19] Bhattacharjee, Sangeeta et al., "Cognitive radio based spectrum sharing models for multicasting in 5G cellular networks: A survey," *Comput. Netw.* 208, 108870, 2022.[19][2]

[20] Gong, L. et al., "Fine-grained trust-based routing algorithm for wireless sensor networks," *Mobile Networks and Applications*, pp. 1-10, 2021.[20][2]

[21] Bharathy, G.T. et al., "Research and development in the networks of cognitive radio: A survey," *Sustainable Communication Networks and Application*, Springer, pp. 475–494, 2021.[2]

[22] Bany Salameh, Haythem et al., "Intelligent secure networking in in-band full-duplex dynamic access networks: Spectrum management and routing protocol," *J. Netw. Syst. Manage.* 29 (2), 1–18, 2021.[2]

[23] Aslam, Muhammad Muzamil et al., "Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges," *Wirel. Commun. Mob. Comput.* 2021.[2]

[24] Amjad, Muhammad Faisal et al., "AdS: An adaptive spectrum sensing technique for survivability under jamming attack in CRSNs," *Comput. Commun.* 172, 25–34, 2021.[2]

[25] S., Sherif, "A Review of Metaheuristic Optimization for Network Traffic Management in Telecommunications," *Metaheuristic Optimization Review*, pp. 01-10, 2025.[2]

[26] Chen, Zhibo et al., "Federated learning-based cooperative spectrum sensing in cognitive radio," *IEEE Commun. Lett.* 26 (2), 330–334, 2021.[2]

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 251-256

[27] Chen, Mingzhe et al., "A joint learning and communications framework for federated learning over wireless networks," *IEEE Trans. Wireless Commun.* 20 (1), 269–283, 2020.[2]

[28] Chen, Zhibo et al., "Deep learning for cooperative spectrum sensing in cognitive radio," *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pp. 741–745, 2020.[2]

[29] Aygül, Mehmet Ali et al., "Spectrum occupancy prediction exploiting time and frequency correlations through 2D-LSTM," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, 2020.[2]

[30] Dhawan, Anshu and Jha, C.K., "Routing and security issues in cognitive radio ad hoc networks (CRAHNs)—a comprehensive survey," *International Conference on Innovative Computing and Communications*, Springer, pp. 489–501, 2020.[2]

[31] Choudhury, Punam Dutta et al., "Big spectrum data and deep learning techniques for cognitive wireless networks," *Deep Learning and Neural Networks: Concepts, Methodologies, Tools, and Applications*, IGI Global, pp. 994–1015, 2020.[2]

[32] Neamatollahi, P. et al., "Hierarchical clustering-task scheduling policy in cluster-based wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1876-1886, 2017.[2]

[33] Aljumah, A. and Ahanger, T.A., "Futuristic method to detect and prevent blackhole attack in wireless sensor networks," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 2, pp. 194, 2017.[2]

[34] Kalkha, H., Satori, H. and Satori, K., "Preventing black hole attack in wireless sensor network using HMM," *Procedia computer science*, vol. 148, pp. 552-561, 2019.[2]

[35] Kumar, D., "Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks," *IET Wireless Sensor Systems*, vol. 4, no. 1, pp. 9-16, 2014.[2]

[36] Belhajem, I., Maissa, Y.B. and Tamtaoui, A., "Improving vehicle localization in a smart city with low cost sensor networks and support vector machines," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 854-863, 2018.[2]

[37] Ahmed, A. et al., "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Frontiers of Computer Science*, vol. 9, pp. 280-296, 2015.[2]

[38] Wang G. et al., "Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce," *IEEE Transactions on Parallel and Distributed Systems*, 2013.[2]

[39] Singh, Kumar Shio et al., "A survey on network security and attack defense mechanism for wireless sensor networks," *International journal of computer trends and technology*, vol.1, no. 2, pp. 9-17, 2011.[2]

[40] Younis, O., & Fahmy, S., "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *Mobile Computing, IEEE Transactions* vol 3, no.4, pp. 366-379, 2004.[2]

[41] Alsaedi N., Hashim F., and Sali A., "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks," *IEEE 12th Malaysia International Conference on Communications (MICC)*, Kuching, Malaysia, 2015.[2]

[42] Prasanna S. and Rao S., "An Overview of Wireless Sensor Networks Applications and Security," *IJSCE*, vol.2, no.2, 2012.[2]

[43] Di Pietro R. et al., "Data security in unattended wireless sensor networks," *IEEE Trans. Comput.*, vol. 58, no. 11, pp. 1500−1511, 2009.[2]

[44] Kaschel H., Mardones J., and Quezada G., "Safety in wireless sensor networks: types of attacks and solutions," *Stud. Informatics Control*, vol. 22, no. 3, pp. 323−329, 2013.

[45] Mangai, S.A., Sankar, B.R. and Alagarsamy, K., "Taylor series prediction of time series data with error propagated by artificial neural network," *International Journal of Computer Applications*, vol.89, no.1, 2014.