STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **x**, Month 202x, pp 0–9.
Published online in International Academic Press (www.IAPress.org)

Protecting Wireless Sensor Networks Against Sybil Attacks

Omar Zenzoum [1,*], Abdelali Elmounadi [2], Hatim Kharraz Aroussi [1]

[1] *Laboratory of Research in Informatics, Faculty of Sciences, Ibn Tofail University, Kénitra, Morocco*
[2] *Department of Computer Science, Ecole Normale Supérieure of Rabat, Mohammed V University in Rabat, Morocco*

Abstract Wireless sensor networks (WSNs) deployed in the Internet of Things (IoT) environments remain vulnerable to Sybil attacks, in which a malicious device forges multiple identities to infiltrate routing structures and compromise data transmission. This vulnerability is particularly severe in hierarchical protocols such as LEACH and its improved variant, the Equitable Distributed Energy (EDE) protocol, where cluster heads (CH) and transfer nodes (TN) play a critical role in data aggregation and transfer. This paper presents Secured-EDE, a secure extension of EDE that incorporates symmetric key authentication, RSSI based detection, controlled CH and TN election, and centralized trust management by the base station (BS). Simulations conducted under advanced Sybil behavior conditions, including node mobility, transmission power variation, HELLO flooding, and packet dropping, demonstrate significant improvements in packet delivery ratio (PDR), energy efficiency and Sybil detection reliability. Secured-EDE effectively prevents malicious nodes from obtaining CH and TN roles and maintains network performance despite adverse conditions. These results confirm the robustness of the proposed method for securing hierarchical WSN deployments.

Keywords IOT, WSN, Sybil Attack, Hierarchical WSN, Leach protocol, EDE protocol, Security, Energy.

DOI: 10.19139/soic-2310-5070-3007

1. Introduction

WSNs have transformed modern life, supported by the rapid expansion of the IoT, connecting smart devices such as home appliances and security systems [1]. Equipped with transceivers and microcontrollers, these devices collect and transmit data to centralized systems, enabling IoT networks to operate securely and continuously without human intervention, while addressing growing connectivity needs.

WSNs are a central component of the IoT, offering various applications including smart cities, healthcare, environmental monitoring, military surveillance, and industrial automation [2]. WSNs are formed by numerous energy-limited sensor nodes deployed across a designated area, which collaborate to transmit detected data to a central base station [3].

Data obtained from sensors must be transmitted securely to the BS. WSNs are exposed to a wide range of attacks that menace the data transmission [4]. When designing security policies, a general structure aims to eliminate all or part of these attacks. Therefore, security policies must ensure the basic requirements of information security, including authentication, confidentiality, integrity, availability, and non-repudiation.

Due to limited battery capacity, energy efficiency is a major challenge in WSN design [5]. Routing schemes based on clustering, like the Low Energy Adaptive Clustering Protocol, have been widely used to improve energy efficiency and extend the lifetime of networks [6],[7]. In the LEACH protocol, cluster heads are responsible for aggregating and transmitting data to the BS, but this function causes high energy consumption, leading to premature node death and network partitioning.

*Correspondence to: Omar Zenzoum (Email: omar.zenzoum@uit.ac.ma). Laboratory of Research in Informatics, Faculty of Sciences, Ibn Tofail University, Kénitra, Morocco.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

To address this limitation, EDE protocol has been introduced [8]. This protocol extends the LEACH protocol by incorporating TNs that operate as relay nodes between CHs and the BS, reducing the transmission charge on CHs and distributing energy consumption more equitably. Although the EDE protocol improves the energy efficiency of LEACH, it remains vulnerable to security threats such as Sybil attacks [9]. In a Sybil attack, a compromised node invents different identities to increase its chances of being elected as a CH or TN, thereby disrupting cluster formation, data aggregation and communication security.

This paper proposes Secured-EDE, an energy-efficient approach designed to protect hierarchical WSNs against Sybil attacks. It integrates symmetric authentication, RSSI similarity, controlled election of CH and TN, and centralized trust management via the BS. The design maintains a balance between robust security and minimal overhead, making it practical for resources constrained devices. Through comprehensive simulation and evaluation, we demonstrate that Secured-EDE significantly enhances resilience and communication reliability under adversarial conditions. The remainder of this paper is organized as follows: Section 2 review related work. In Section 3, we present the proposed approach. The simulation and results are discussed in Section 4. Finally, Section 5 concludes this work and presents future perspectives.

2. Related work

LEACH is a widely used clustering protocol in wireless sensor networks, designed to minimize energy consumption by periodically rotating cluster heads [10],[11]. Despite its effectiveness, the strong dependence on CHs often leads to rapid energy consumption. Furthermore, the random selection process and the absence of security mechanisms in Leach protocol make it vulnerable to attacks.

EDE improves LEACH by introducing TNs, which act as intermediate nodes between CHs and the BS, in order to reduce the communication charge and ensure a more equitable use of energy over the entire network [8]. However, EDE and similar protocols remain vulnerable without integrated security mechanisms.

A Sybil attack occurs in a WSN when a malicious node illegitimately claims various identities inside the network, creating new ones or stealing those of legitimate nodes [12]. In this way, the attacker can disrupt normal operations such as clustering, routing, and data aggregation, by leading other nodes to treat the attacker as multiple trusted nodes. This manipulation allows the attacker to gain considerable influence, degrade network performance, distort routing decisions and compromise data integrity. As a result, the security, reliability, and efficiency of the WSN are compromised.

Several studies have proposed mechanisms to detect and prevent Sybil attacks. In [13], the authors proposed a lightweight authentication mechanism based on elliptic curve cryptography, which offers high security with keys that are much smaller than those used by RSA or ElGamal. Although this approach offers an effective solution to counter Sybil attacks with reduced computational and energy costs, it still requires asymmetric cryptographic operations that can be heavy for very low-power nodes and introduce latency during key generation or verification.

Amado et al. [14] proposed SybilGuard to secure IoT-based healthcare systems by combining lightweight authentication and encryption. A lightweight prime-order grouping approach encrypts smart health records to verify node identities and protect data confidentiality. This approach, coupled with anomaly-based Sybil detection, strengthens trust and mitigates routing disruptions in smart healthcare environments. However, its effectiveness depends on accurate anomaly detection, and additional cryptographic operations may still introduce latency or overhead for medical devices with very limited resources.

In [15], Gill and al. proposed a coordinator-node-based strategy to protect LEACH from Hello flood attacks. Each advertisement received by a node is forwarded to a coordinator node and then to the base station, which computes connectivity to identify malicious nodes exceeding a threshold. But this approach imposes an extra communication and processing load on the coordinator nodes, creates a potential single point of failure, and can lead to detection delays or reduced accuracy in cases of high network dynamics or node mobility.

A study published in [16]proposes a multimodal biometric authentication system based on RSSI, combining palm print and fingerprint characteristics to verify the authenticity of nodes despite the absence of centralized

network control. However, this method still requires additional processing of biometric data, which can increase cost and complexity.

Fang and al. [17] present a comprehensive survey of trust-based security mechanisms for wireless sensor networks, highlighting their role in detecting and mitigating internal attacks that cryptographic methods cannot prevent. The authors describe a generic trust management system encompassing the collection, storage, modeling, transfer, and decision-making of trust values derived from nodes' behaviors and interactions. They review numerous schemes, such as RFSN, BRSN, EDTM, BTRES, and HTMS, that integrate direct and indirect observations, statistical models, and energy consumption considerations to isolate malicious nodes and secure routing or data aggregation. However, they note that issues like threshold selection, reliance on indirect information, and computational overhead remain key limitations for resource-constrained wireless sensor networks.

While individual strategies are effective to varying degrees, a comprehensive approach combining energy efficiency and multi-level security is essential to ensure the reliable and secure operation of wireless sensor networks in IoT implementations. The following section presents our proposed method that addresses the limitations of the previously cited mechanisms.

3. Proposed approach

Our proposed approach enhances the LEACH protocol by integrating TNs with security mechanisms to prevent Sybil attacks. The TNs optimize the power consumption of cluster heads by relaying aggregated data to the base station. This not only extends network lifetime but also ensures a more balanced energy distribution. To secure the network, we propose an efficient method incorporating symmetric key authentication, controlled election of CH and TN by the BS, detection based on RSSI and centralized trust computation. This ensures resistance to impersonation, forgery, collusion, and replay attacks while remaining efficient in communication.

3.1. Symmetric key Authentication

Before deployment, each sensor node i is provided with a unique symmetric key K_i shared only with the BS. In order to secure communication between nodes, each pair of nodes i and j derives a symmetric pairwise key $K_{i,j}$ as follows:

$$K_{i,j} = H(K_i \,\|\, K_j)$$

Where $H(\cdot)$ is a hash function and $\|$ denotes concatenation. This design avoids explicit key exchanges and eliminates the exposure of confidential information during execution. Each node maintains an outgoing counter C_i and incoming counters C_j per neighbor, which provides replay protection for all communications. A packet transmitted from node i to neighbor j includes the sender and receiver identifiers, the sender counter, the message, and a message authentication code (MAC). The packet structure is expressed as:

$$\text{Packet} = \{ID_{\text{src}},\ ID_{\text{dst}},\ C,\ m,\ MAC\}$$

The MAC is calculated using the key $K_{i,j}$, the counter value, and the fields of the protected message, in accordance with:

$$MAC_{i,j}(m) = H(K_{i,j} \,\|\, C_i \,\|\, m)$$

The receiving node verifies the MAC using its pairwise key and only accepts the packet when the counter is strictly greater than the last value recorded for that sender. This ensures integrity, authenticity and freshness of the message with minimal computing overhead. All communications originating from the BS, including updates such as blacklists or trusted node lists (TNL), are sent individually to each node via unicast using the symmetric key of the node. This prevents any node from falsifying BS messages or usurping network authority, even if some nodes are compromised.

3.2. CH and TN Election

The selection of CH and TN is controlled by the BS in order to maintain the network security. At the beginning of each cycle, nodes that decide to assume the role of CH or TN submit a request to the BS. The BS evaluates these requests, ensuring that each node has a high level of trust and has not been reported as a suspicious Sybil node. After processing all requests, the BS produces a trusted node list containing the nodes authorized to act as CH or TN in the current round. This list is then distributed individually to each node in the network. During cluster formation, nodes only accept CH or TN announcements from nodes listed in the TNL.

This approach ensures that only nodes approved by BS can assume critical roles in the network, thereby preventing Sybil nodes or compromised nodes from disrupting network operations.

3.3. Monitoring of cluster members and RSSI based detection by the CH

Each CH performs local Sybil detection by comparing the RSSI signatures of its members. Identities belonging to the same physical device tend to have highly correlated signal characteristics. For any nodes j and k, the CH calculates the normalized RSSI similarity $R_i(j,k)$. If this value exceeds a threshold, the pair is flagged as Sybil suspicious. Detection is based on the relative similarity between nodes in the same cluster, which inherently mitigates the impact of multipath fading, moderate mobility, and environmental noise, thereby improving the stability of the physical layer fingerprinting process. Suspicious pairs contribute to the binary Sybil indicator $R_i(r)$ sent to the BS at the end of the round. The threshold of $\Theta = 0.85$ is selected to ensure that only nodes with a very high RSSI similarity are considered suspicious. This value effectively distinguishes Sybil nodes from legitimate nodes, minimizing false positives (FP) while maintaining detection accuracy. In addition to physical interconnection, each CH continuously monitors the behavior of its members, including packet forwarding, message repetition, and authentication consistency, to detect any potentially malicious activity. These behaviors are captured using three binary indicators per node: a bad behavior indicator reflecting any detected malicious activity, a good behavior indicator representing correct participation, and a Sybil indicator derived from RSSI similarity analysis.

3.4. Trust Management at the BS

At each round r, every CH reports the status of its cluster members to the BS using three binary indicators for each node $i : R_i(r) \in \{0,1\}$ for suspected Sybil attacks, $i : M_i(r) \in \{0,1\}$ for misbehaving, and $i : G_i(r) \in \{0,1\}$ for good behavior. Initially, the trust score of the each node is set to $T_i(0) = T_{\text{init}} = 1$, and then it is dynamically updated based on the observed behavior of the node in the range of $[0,1]$. After collecting these reports from all CHs, the BS updates the trust value for each node according to the following formula:

$$T_{\text{BS}}(i, r+1) = \min\left(1,\, \max\left(0,\, T_{\text{BS}}(i,r) + \alpha G_i(r) - \beta M_i(r) - \rho R_i(r)\right)\right)$$

With parameters $\alpha = 0.05$, $\beta = 0.10$, and $\rho = 0.15$. This formulation allows nodes to gradually recovery of trust while quickly penalizing detected malicious behavior. Nodes whose trust falls below Tmin are placed on the global blacklist. $T_{\min} = 0.5$ has been chosen to represent the neutral midpoint, allowing honest nodes to gradually recover while nodes whose trust clearly falls below the safety threshold are quickly blacklisted.

3.5. Blacklist update

The blacklist is distributed through authenticated messages from the base station. Whenever new Sybil nodes are detected, the base station sends the following message individually to each node:

$$\text{BL\_UPDATE} = \{ID_{\text{BS}},\ ID_{\text{dst}},\ ID_{\text{suspect1}},\ ID_{\text{suspect2}},\ \ldots,\ C_{\text{BS}},\ MAC_{\text{BS}}\}$$

Each receiving node verifies the MAC to ensure the authenticity of the message, and updates its local blacklist only after a successful verification. This approach guarantees tamper resistance, effective detection and exclusion of Sybil attacks, protection against replay attacks, and maintains network consistency.

4. 4. Simulation and evaluation

To evaluate Secured-EDE, we compare it to the EDE protocol. Secured-EDE retains the hierarchical clustering of EDE while incorporating security mechanisms. This comparison highlights improvements in energy stability, network lifetime, cluster security, and resistance to sybil attacks, using identical network parameters to ensure uniform results.

4.1. Simulation scenarios

The proposed approach was implemented in Python and simulated on Google Colab to evaluate its performance under various network and attack conditions. First, a default simulation scenario was selected to illustrate the figures in this section. This scenario provides a detailed view of topology changes, energy consumption, packet delivery performance and Sybil detection accuracy. To ensure that the results are statistically valid and generalizable, the simulation was run 30 times using independent Monte Carlo experiments. In addition, we run other experiments with different network sizes and densities, summarized in Table 2, to evaluate scalability. In the main scenario, a network of 100 nodes was randomly distributed in a 100 m × 100 m area. The initial energy of nodes was fixed in 2 Joules. The simulation was run for 50 rounds and repeated over 30 independent runs to ensure statistical reliability. Sybil nodes ranged from 5 nodes to 10% of the total number of nodes in the network and acted as sophisticated mobile attackers by generating multiple fake identities, varying their transmission power to false RSSI readings, broadcasting excessive HELLO messages, forging packets, and dropping packets. Sybil nodes may sometimes behave normally in order to simulate an escape strategy. Both the classic EDE and Secured-EDE protocols were tested to provide a clear comparative analysis. The evaluation metrics include energy consumption, packet delivery rate, detection rate, false positives, and dead nodes. Table 1 below summarizes the simulation parameters.

Table 1. Simulation Parameters

Parameter	**Value**
Field size	$100\,\text{m} \times 100\,\text{m}$
Base station position	Field size / 2, Field size + 20
Number of nodes	100 100 including 10% as Sybil nodes
Fake identities per Sybil node	5
Initial node energy	2 Joule
Data packet size	4000 bits
Number of rounds	50
Monte Carlo runs	30

4.2. Simulation Results

In the following, we depict the simulation of EDE and Secured-EDE under Sybil attack. Fig. 1 shows the topology created during the first round of the first run. The BS is represented by a yellow square. Legitimate nodes appear as blue circles. CHs are represented by red circles, TNs by green circles, and attackers by red Xs.

Fig. 2 illustrates the network topology in the last round, where black Xs indicate mobile Sybil nodes that have been detected and isolated from the network. This ensures that no malicious nodes stay connected or able to join clusters or disrupt routing. The result demonstrates that Sybil nodes are detected early, allowing the network to be stable for the remainder of the simulation.

Fig. 3 compares the energy consumption of EDE and Secured-EDE during simulation rounds. Even with additional security operations, Secured-EDE consumes less total energy than EDE. Average energy consumption is 15.27% with Secured-EDE, compared to 16.77% for EDE under the same attacks. The higher consumption of EDE is due to Sybil nodes that disrupt clustering and drains the energy of legitimate nodes, which are forced to process an excessive number of fake HELLO messages, forged packets, and replay attempts. In Secured-EDE, early detection balances the network, reduces unnecessary transmissions, and improves overall efficiency.

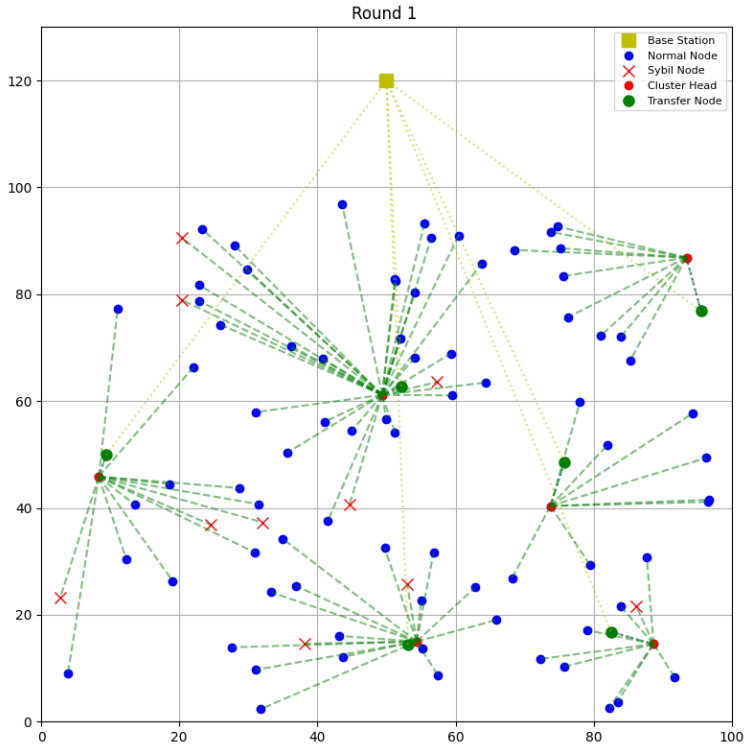

Figure 1. Figure 1. The network topology created at the first round.

Although security mechanisms involve additional computing and communication costs, these are compensated by the elimination of energy waste caused by processing malicious traffic. As a result, the network operates more efficiently and legitimate nodes save energy over time.

The packet delivery performance is illustrated in Fig. 4, where the PDR of the two protocols is compared. In the classic EDE configuration, Sybil attackers are elected multiple times to the CH and TN roles and drop a large portion of the aggregated packets. As a result, the PDR decreases 53.95%, revealing a serious disruption in network reliability. When Secured-EDE is applied, the PDR increases significantly to 97.03%, reflecting highly reliable transmission conditions. The packet loss, displayed simultaneously, decreases significantly under Secured-EDE and remains stable once Sybil nodes are eliminated. This figure therefore demonstrates the significant contribution of secure CH and TN election, identity verification, and trust management in maintaining continuous data transmission, even in difficult environments.

The strategic behavior of Sybil nodes during CH and TN elections is examined in more detail in Fig. 5, which illustrates the average frequency with which attacking nodes assume these critical roles. In the classic EDE protocol, Sybil nodes often succeed in being elected as CH or TN, exploiting their falsified identities to dominate cluster formation and compromise transfer operations. With Secured-EDE, Sybil nodes never succeed in obtaining CH or TN roles at any time during the simulation. The controlled election process and trust indicators reported by the CHs effectively prevent adversaries from changing the network hierarchy. As a result, Fig. 5 demonstrates that Secured-EDE maintains strong structural resilience against Sybil attacks.

Fig. 6 below illustrates the evolution of the detection process and shows that all Sybil attackers were identified within the early rounds. After this initial phase, all detected Sybil nodes were successfully excluded from participating in the network. The absence of false positives in all rounds confirms the effectiveness of the detection strategy, which combines trust management, RSSI similarity and behavioral indicators. The early detection illustrated in Fig. 6 shows that the security mechanism quickly stabilizes the network and prevents long-term degradation, demonstrating the robustness and responsiveness of Secured-EDE.

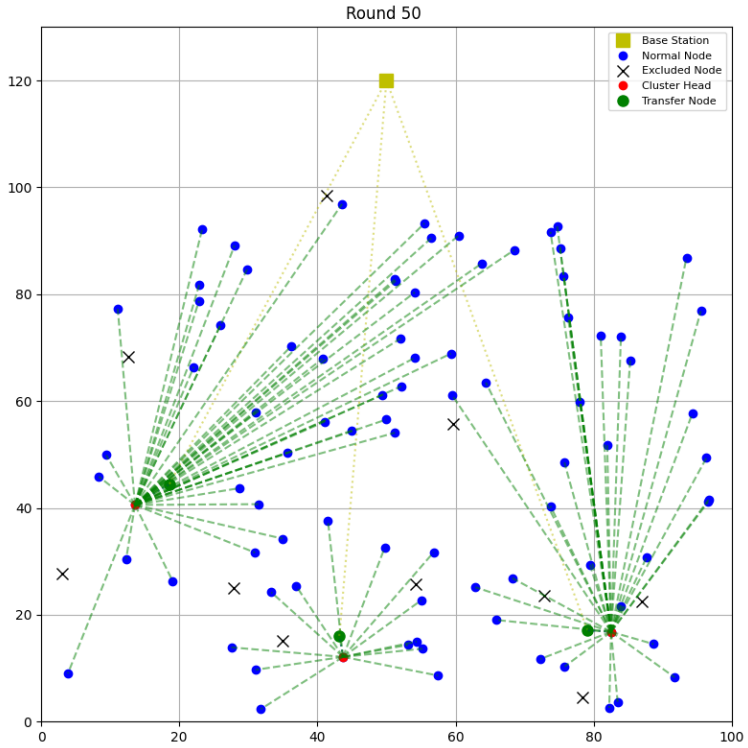

Figure 2. Figure. 2 The network topology at the end of the simulation basing on Secured-EDE.

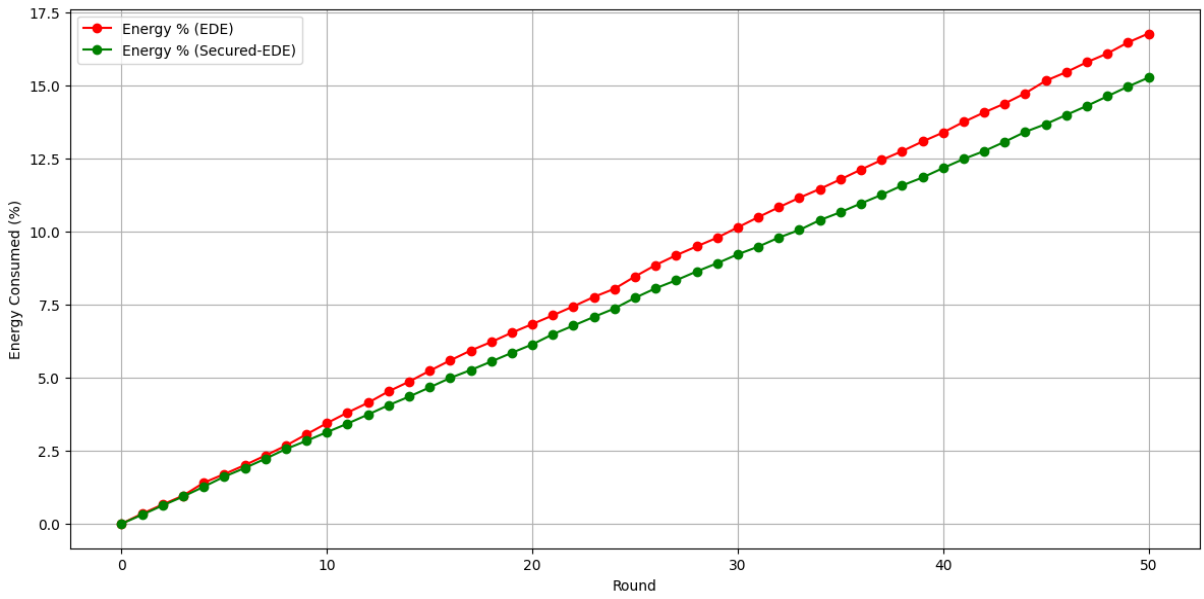

Figure 3. Figure 3. Energy consumption evolution over rounds.

Collectively, these figures present a clear and consistent result. While the classic EDE protocol collapses under Sybil attacks, Secured-EDE preserve energy stability, protects hierarchical roles, ensures reliable data delivery and effectively isolates malicious nodes.

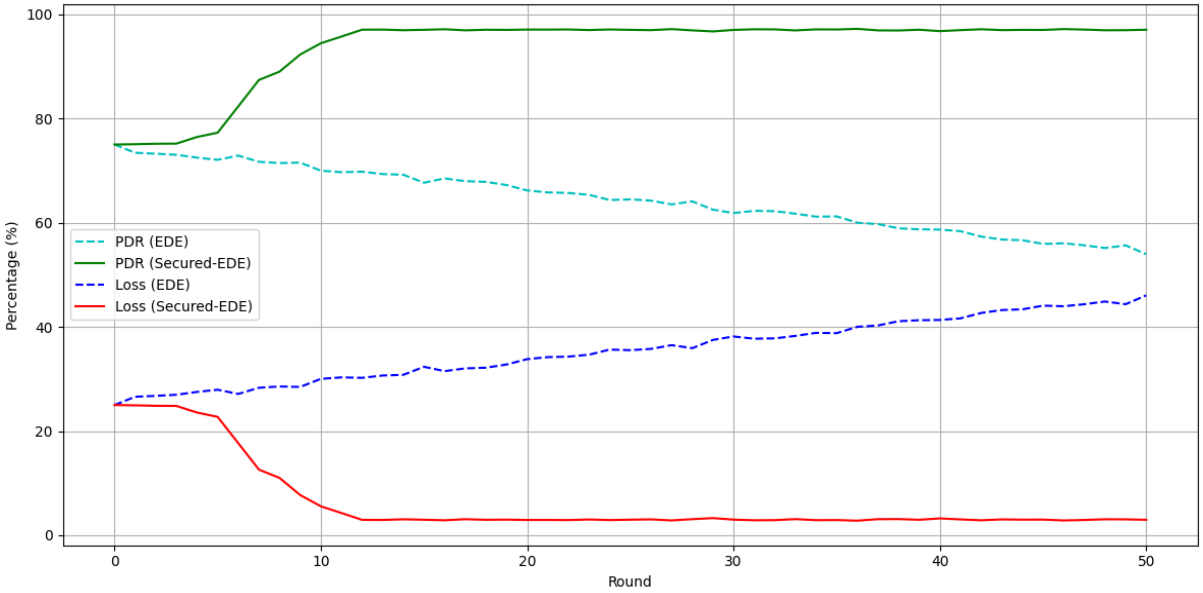

Figure 4. Figure 4. Evolution of th PDR and the packet loss over time.

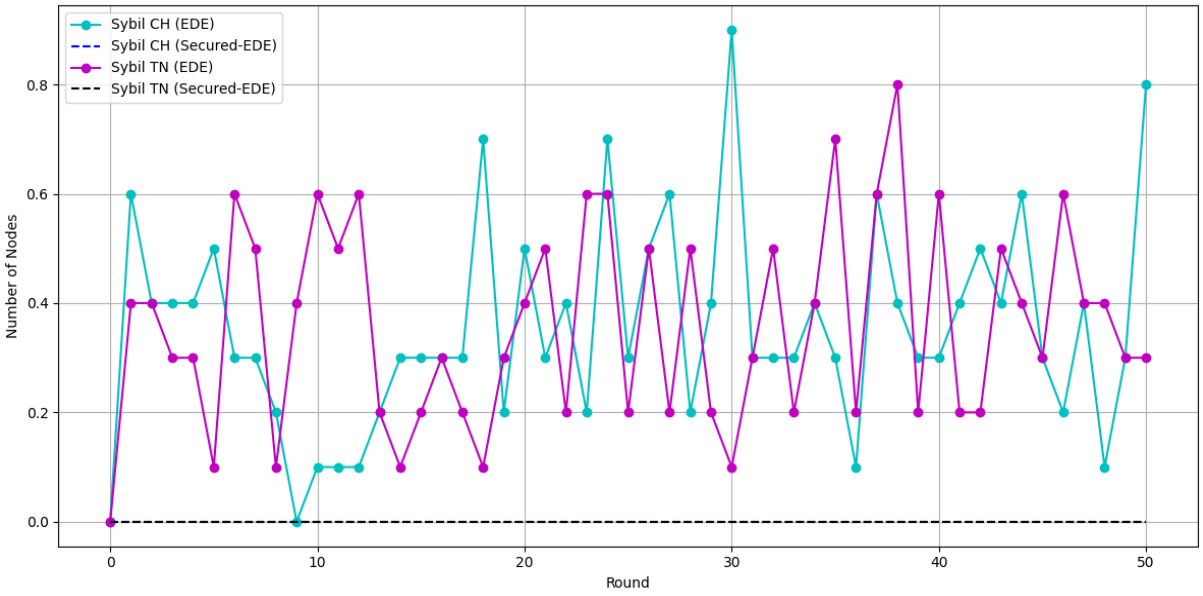

Figure 5. Figure 5. Average number of times Sybil nodes were assigned as CHs and TNs in each round.

4.3. Discussion and Evaluation

The proposed method was evaluated not only on networks of fixed size, but also on networks of varying densities and sizes. Table 2 presents the results obtained for networks comprising between 100 and 500 nodes and areas of 100 × 100 m and 200 × 200 m. Even with longer communication distances and higher collision risks in larger networks, Secured-EDE guarantees effective detection and maintains a PDR of around 95%. Energy consumption naturally increases with larger fields, but the method remains more efficient than traditional EDE because it avoids

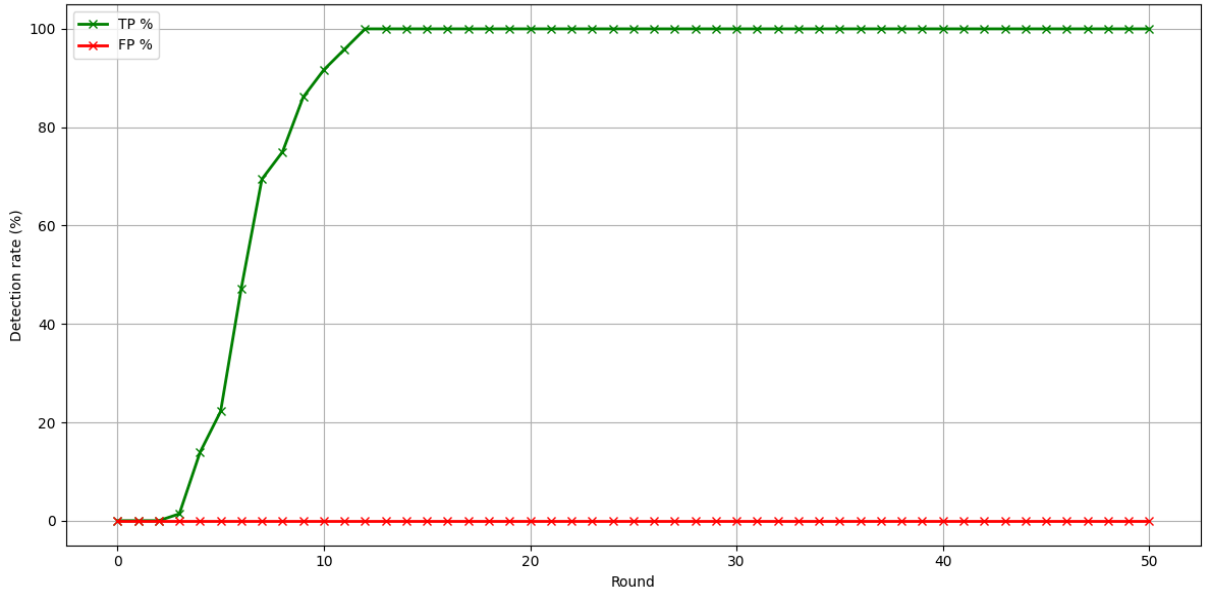

Figure 6. Figure 6. Detection of Sybil attackers across rounds using the proposed approach.

retransmissions caused by Sybil attacks and unstable clusters. Dead nodes remain very few in all cases, showing that stable CH and TN rotation and elimination of malicious nodes help maintain node lifetime and network availability. These results show that the method works well even as the network grows larger or becomes sparser.

Table 2. Comparison of simulations on networks with different sizes and densities

Number of Nodes	Field size	Energy consumed	PDR	Detection Rate	Dead nodes
100	100×100	30.53 J	97.03%	100%	0%
100	200×200	94.12 J	94.8%	100%	2.80%
200	100×100	44.66 J	96.1%	100%	0%
200	200×200	121.46 J	95.5%	100%	1%
500	200×200	261.54 J	95.2%	100%	0.52%

The overhead imposed by security mechanisms remains reasonable for low-power wireless sensor networks. The computational costs are low, as symmetric key authentication relies on lightweight hashing operations. Communication costs are reasonable, including CH and TN role requests, occasional blacklist update, and monitoring of cluster members by each CH, which sends one report per round to the BS. This supervision introduces a slight increase in computing and energy costs. However, this is minimal, as the number of CHs in each cycle is typically very small. Storage requirements are limited for standard sensor nodes, which store their symmetric key, a small set of paired keys, replay counters, a minimal TNL and blacklist entries. To reduce the security overhead on the nodes, the base station performs all trust evaluations and blacklist updates. Overall, the combined costs of computation, communication and storage are reasonable compared to the significant gains in reliability and security offered by the Secured-EDE. In summary, Secured-EDE offers balanced energy efficiency, detection accuracy and communication reliability. Unlike LEACH and EDE, it effectively isolates Sybil nodes and prevents compromised nodes from playing a critical role. The additional overhead for communication and computation is minimal compared to the gains in network performance, demonstrating that Secured-EDE is suitable for real-world WSN deployments while providing protection against advanced Sybil attacks.

5. Conclusion

In this paper, we proposed Secured-EDE, a secure and energy-efficient clustering approach for WSNs in IoT applications. By enhancing the Leach protocol with Transfer Nodes and integrating symmetric key authentication, RSSI-based detection, controlled CH and TN election, and centralized trust computation and evaluation performed by the BS, we addressed both energy efficiency and security challenges. Secured-EDE ensures robust identity validation and protection against manipulation of routing and aggregation processes. The simulation, based on Monte Carlo runs, demonstrated significant improvements in PDR, energy efficiency and detection accuracy. Sybil attackers were consistently detected early, prevented from assuming CH or TN roles, and completely excluded from the routing process, thereby enabling reliable and continuous network operation. Future work will focus on improving CH and TN selection to support networks with high density without overloading the BS or reducing responsiveness, ensuring the long-term scalability and applicability of Secured-EDE in difficult IoT environments. In addition, we plan to validate the approach on real sensor platforms using Contiki or TinyOS to provide practical feedback under real-world conditions. Another key direction is to extend the approach to resist combined attacks, including Sybil, wormhole, and blackhole attacks.

REFERENCES

1. Kamal Gulati, Raja Sarath Kumar Boddu, Dhiraj Kapila, Sunil L Bangare, Neeraj Chandnani, and G Saravanan. A review paper on wireless sensor network techniques in internet of things (iot). *Materials Today: Proceedings*, 51:161–165, 2022.
2. Luca Mainetti, Luigi Patrono, and Antonio Vilei. Evolution of wireless sensor networks towards the internet of things: A survey. In *SoftCOM 2011, 19th international conference on software, telecommunications and computer networks*, pages 1–6. IEEE, 2011.
3. Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.
4. Zhang Huanan, Xing Suping, and Wang Jiannan. Security and application of wireless sensor network. *Procedia Computer Science*, 183:486–492, 2021.
5. R Ramya and Thomas Brindha. A comprehensive review on optimal cluster head selection in wsn-iot. *Advances in Engineering Software*, 171:103170, 2022.
6. M Mehdi Afsar and Mohammad-H Tayarani-N. Clustering in sensor networks: A literature survey. *Journal of Network and Computer applications*, 46:198–226, 2014.
7. Klidbary S Haghzad, M Javadian, et al. Improvement of low energy adaptive clustering hierarchical protocol based on genetic algorithm to increase network lifetime of wireless sensor network. 2024.
8. Yassine Rayri, Hatim Kharraz Aroussi, and Abdelaziz Mouloudi. Energy management in wsns. In *International Conference on Artificial Intelligence and Symbolic Computation*, pages 127–136. Springer, 2019.
9. Ahmet Oztoprak, Reza Hassanpour, Aysegul Ozkan, and Kasim Oztoprak. Security challenges, mitigation strategies, and future trends in wireless sensor networks: A review. *ACM Computing Surveys*, 57(4):1–29, 2024.
10. Sudhanshu Tyagi and Neeraj Kumar. A systematic review on clustering and routing techniques based upon leach protocol for wireless sensor networks. *Journal of Network and Computer Applications*, 36(2):623–645, 2013.
11. Sunil Kumar Singh, Prabhat Kumar, and Jyoti Prakash Singh. A survey on successors of leach protocol. *Ieee Access*, 5:4298–4328, 2017.
12. Haomeng Xie, Zheng Yan, Zhen Yao, and Mohammed Atiquzzaman. Data collection for security measurement in wireless sensor networks: A survey. *IEEE Internet of Things Journal*, 6(2):2205–2224, 2018.
13. Amado Illy, Youssou Faye, and Tiguiane Yelemou. Lightweight authentication system for software-defined wireless sensor networks. In *International Conference on e-Infrastructure and e-Services for Developing Countries*, pages 155–162. Springer, 2023.
14. Jie Li and ZhanJun Wang. Sybil attack detection for secure iot-based smart healthcare environments. *Journal of The Institution of Engineers (India): Series B*, 105(6):1557–1569, 2024.
15. Reenkamal Kaur Gill and Monika Sachdeva. Detection of hello flood attack on leach in wireless sensor networks. In *Next-Generation Networks: Proceedings of CSI-2015*, pages 377–387. Springer, 2017.
16. NV Brindha and VS Meenakshi. An rssi-based sybil attack detection system with continuous authentication using a novel lightweight multimodal biometrics. *International Journal of Intelligent Unmanned Systems*, 10(1):3–21, 2022.
17. Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. Trust-based attack and defense in wireless sensor networks: a survey. *Wireless Communications and Mobile Computing*, 2020(1):2643546, 2020.