

ORIGINAL RESEARCH

Open access

Innovative Security Framework for Wireless Sensor Network Applications in Smart Grids

Sven Larsson^{1*}, Erik Johansson¹, Anna Nilsson²

Abstract

The Smart Grid (SG) seeks to overcome the limitations of conventional power systems by integrating renewable energy sources. It leverages wireless sensor networks (WSNs) to improve monitoring of power generation equipment. However, the open and expansive deployment of WSNs in SG introduces new vulnerabilities and potential attacks. This paper introduces a novel security framework for WSNs in SG that utilizes public key infrastructure (PKI). The core concept involves distributing the duties of the certification authority (CA) across multiple sensor nodes to guarantee service availability and scalability. A new lightweight clustering method is developed to select these nodes, accounting for their trust values and remaining energy. This framework delivers essential security features, including authentication and data confidentiality, while countering threats such as Sybil attacks and eavesdropping. Comprehensive simulations with OMNET++ and the Castalia framework demonstrate the clustering algorithm's effectiveness: nearly all sensors join clusters, and the number of cluster heads remains consistent even when malicious nodes are present, highlighting the framework's resilience.

Keywords Smart Grid (SG), Wireless sensor networks (WSNs), Public key infrastructure (PKI), Clustering, Certification authority (CA)

*Correspondence:

Sven Larsson
sven.larsson@kth.se

¹ Department of Smart Electrical Systems, Faculty of Engineering, KTH Royal Institute of Technology, Stockholm, Sweden

² Department of Energy Analytics and Optimization, Faculty of Engineering, Lund University, Lund, Sweden

Introduction

Background

Over the past few decades, environmental concerns have prompted governments worldwide to modernize traditional electrical grids into smart grids. The conventional grid has several shortcomings: it relies heavily on nonrenewable resources, contributing to greenhouse gas emissions and climate change; it generates excess energy that cannot be stored, leading to significant waste; and it lacks sophisticated communication and monitoring capabilities [1]. The SG aims to enhance the efficiency, adaptability, and dependability of electricity systems [2]. A defining characteristic of SG is the incorporation of renewable energy sources, such as photovoltaic power systems (PPS), which can be installed on building rooftops or in large solar farms. SG employs diverse communication technologies, both wired and wireless, enabling grid components, such as generators and substations, to exchange data while meeting critical requirements, including low latency, high reliability, sufficient bandwidth, security, privacy, scalability, and interoperability. Because energy generators are often placed in remote or challenging environments, maintenance and real-time oversight become difficult. These installations face risks including fire damage, ice accumulation, and electrical hazards. WSNs offer an effective solution for monitoring in such demanding conditions where human intervention is impractical. Their primary

functions include tracking and environmental monitoring [3]. WSNs facilitate the collection and sharing of data on parameters like humidity, voltage, and temperature, enabling prompt detection of issues. They stand out due to simple deployment, affordability, and broad coverage compared to conventional wireless systems [4].

Problem statement

The integration of varied communication technologies in SG heightens security risks. Securing WSN-based applications in SG is particularly challenging due to the open architecture of WSNs, which exposes them to attacks such as Denial-of-Service (DoS), selective forwarding, sinkhole, and Sybil attacks [5]. WSNs are commonly used across extensive solar and wind installations, yet most research on SG security has concentrated on the consumer side, largely overlooking the power generation side. Any internal or external attack on these WSNs must not disrupt SG operations or energy production. Therefore, security remains a vital concern, requiring fulfillment of multiple objectives: non-repudiation (preventing nodes from denying their actions), integrity (ensuring data remains unaltered), authentication (verifying node identities), and confidentiality (protecting sensitive information) [5, 6].

Existing security approaches for WSNs in SG fall into two categories: encryption-based and non-encryption-based. Non-encryption methods address only limited threats and offer partial protection. Encryption-based solutions, however, defend against a wider range of attacks and support comprehensive security services. Public key infrastructure (PKI) is a robust option that meets most security needs in WSNs for SG [5]. It supports digital signatures for authentication and non-repudiation, keyed hash functions for integrity, and encryption for confidentiality [6]. Nevertheless, traditional PKI faces challenges in availability and scalability because of its centralized design. The CA becomes a single point of failure; if compromised, the entire network is affected, and it struggles to handle large numbers of sensors efficiently, regardless of network size.

Contribution

To overcome the drawbacks of centralized PKI, this study presents a distributed PKI architecture tailored for WSN applications in SG. The design relies on a clustering approach in which cluster heads (CHs) assume the CA's responsibilities within their respective clusters. This delegation enhances both scalability and service availability. Previous PKI schemes for WSNs typically rely on either a fixed centralized CA [7, 8] or a pre-selected group of authorities configured offline [9, 10]. Both strategies still suffer from a single point of failure. The proposed solution dynamically elects sensor nodes to serve as CAs, ensuring that compromise of one affects only its local cluster.

The election process uses a newly designed clustering algorithm that incorporates multiple factors: node energy levels, number of trustworthy neighbors, and trust metrics. This algorithm was developed because existing methods are often too resource-intensive for large-scale SG deployments or rely solely on location or energy, which are insufficient for selecting reliable CHs and forming balanced clusters. Trustworthiness is essential since CHs act as CAs. Trust metrics, combined with energy and neighbor reliability, promote cluster stability—trustworthy neighbors can step in if a CH fails. The algorithm also aims to achieve balanced cluster sizes to evenly distribute the workload. While many clustering protocols exist, none fully combine all these required characteristics.

Key contributions of this work include:

- Development of a novel clustering algorithm for CH selection that evaluates trust metrics, trustworthy neighbors, energy levels, and cluster size to ensure balanced and secure clusters.
- Design of a distributed PKI where CHs function as CAs and registration authorities (RAs) verify node authenticity before certification.
- Evaluation of the clustering performance and overall architecture robustness through simulations.

Security in WSN-Based SG Attacks

WSNs are susceptible to various attacks across network layers [11]. This work specifically addresses the following:

DoS attack

Limited processing power and memory make WSNs vulnerable to DoS attacks that render network resources unavailable. In a PKI context, such attacks can target the CA and disrupt the certification process [5].

Sinkhole attack

An adversary introduces a counterfeit node or compromises an existing one to attract and intercept network traffic. The malicious node can then drop, modify, or delete data. Robust authentication mechanisms are necessary to prevent this [5].

Sybil attack

A malicious node assumes multiple identities to disrupt routing and communication. Effective identity management is required to mitigate this threat [5].

Traffic analysis attack

Attackers monitor communication patterns through eavesdropping to deduce network topology and locate critical nodes, potentially enabling additional attacks, such as DoS. Strong asymmetric encryption serves as the primary defense against eavesdropping [11].

Related work

Security solutions for WSN-based applications in Smart Grids have received considerable attention in recent years. In [2], the authors introduced a framework designed to identify DoS attacks and stop them from reaching the sink node. Their approach identifies and blocks potentially malicious nodes by comparing the time interval between consecutive requests against a set threshold. Blocked nodes have their access records stored, and repeated requests increase a counter to confirm suspicion. However, this method has a notable drawback: legitimate nodes may be incorrectly blocked if they happen to send a few requests within a short time window.

The authors in [12] developed an adaptive, channel-aware system to detect selective forwarding attacks in WSNs. Their solution divides the network lifetime into evaluation periods and calculates the expected normal packet loss rate for each period based on radio link quality. In the first phase, baseline packet loss is estimated; in the second, nodes periodically assess their neighbors' reputation; and in the third, each node calculates the attack probability of its neighbors and shares the results. A key limitation is that the scheme relies on a non-encryption-based technique, which fails to deliver the full range of security services required in WSNs and SG environments.

Alfandi et al. [7] presented a hybrid cryptography scheme that uses public-key cryptography to ensure confidentiality and integrity during data transmission between sensor nodes. In their approach, a central CA signs each node's public key and network address, then redistributes the key, address, and signature. Nodes perform a certificate-based handshake to generate symmetric keys for subsequent communication. The main weakness is the reliance on a central CA, which creates a single point of failure.

Nandini and Praveenkumar [8] proposed a PKI implementation for SG using wireless networks. During registration, a digital signature binds a user's identity to its public key. A Registration Authority (RA) verifies this binding, after which the CA issues the certificate. Secure access begins with a Certificate Signing Request (CSR) sent to the RA, and a validation

authority informs relying parties (RPs) of the certificate's status. Like previous schemes, the centralized CA remains a single point of failure.

In Ref. [9], the authors introduced a hierarchical PKI for SG with five levels. The top “master level” serves as the root of trust, issuing certificates to the level below, while its public key is known to all devices. Lower levels have progressively shorter validity periods and narrower responsibilities, with the bottom level unable to issue certificates. The critical shortcoming is that the master level constitutes a single point of failure for the entire system.

The work in Ref. [10] sought to enhance existing PKI in SG by dividing the grid into groups based on a hierarchical communication structure, thereby distributing the Trust Authority (TA) and addressing the single point of failure issue.

For WSNs deployed in Smart Grids, the PKI must remain robust regardless of network size or the number of sensor nodes. In this paper, we introduce a new distributed PKI for WSN-based SG applications that uses a clustering algorithm to dynamically elect suitable sensor nodes to act as CAs within their clusters. This election considers network topology and additional parameters to ensure the PKI's stability and scalability. The following section reviews selected clustering algorithms in WSNs.

Clustering Protocols in WSNs

Classification of clustering protocols in WSNs

Clustering protocols in WSNs can be categorized in various ways depending on different criteria [13, 14]. Numerous studies have contributed to the evolution of these algorithms over the years. In [13], clustering algorithms are divided into probabilistic and non-probabilistic categories. The authors in Ref. [15] classify cluster-based routing protocols based on macro and micro parameters. Another classification in Ref. [16] groups them into probabilistic, deterministic, and preset approaches. In Ref. [17], the authors propose seven categories: connected dominated set-based, mobility-aware, energy-efficient, load-balancing, dynamic, and homogeneous/heterogeneous. In Ref. [18], clustering algorithms are organized into four classes: homogeneous-node, heterogeneous-node, fuzzy-logic-based, and heuristic-based methods.

In this section, we present a comprehensive new classification of clustering algorithms in WSNs based on the following criteria:

- Probabilistic vs. Non-probabilistic clustering: In probabilistic methods, each sensor node is assigned a probability value, which serves as the primary criterion for selecting a cluster head [13, 19]. In non-probabilistic approaches, CH election relies on multiple specific factors such as node location, number of neighbors, and security-related metrics [13, 20].
- Clustering in homogeneous vs. heterogeneous networks: In homogeneous networks, all nodes at the same level have identical initial energy, sensing capabilities, and communication ranges. Therefore, any node can become a CH, and algorithms are typically energy-based or hybrid parameter-based [14]. In heterogeneous networks, nodes vary significantly in resources, energy, and processing power. They are usually divided into super-nodes (with superior hardware and capabilities) and normal nodes. CHs are generally selected from super-nodes. These networks also use either energy-based or hybrid-parameter-based selection methods [14].
- Energy-based clustering: These algorithms prioritize the sensor node with the highest remaining energy level as the optimal choice for cluster head in heterogeneous environments [14].
- Hybrid parameters-based clustering: CH selection considers multiple factors simultaneously, including cluster size, neighbor information, distance to the base station, and others [14].

The next section reviews several existing clustering algorithms and classifies them by their methodologies and the parameters they employ.

Related work

Numerous researchers have developed clustering algorithms for WSNs and explored their benefits across different domains, including security. The following section discusses several notable studies in this area.

Zahedi [19] focused on the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. The original LEACH selects cluster heads randomly using a threshold equation without considering node energy levels. To address this, the authors modified the threshold equation by incorporating the ratio of remaining energy to the initial maximum energy, resulting in an improved version of LEACH.

The authors in Ref. [21] introduced a clustering algorithm that selects CHs based on a combination of a trust metric and several other factors. The trust metric is behavior-based and derived from both direct and indirect observations. It considers parameters such as the rate of acknowledged packets, the successful packet delivery ratio, the data forwarding ratio, and node availability. Additional metrics used for CH election include node waiting time, connectivity degree, and relative mobility.

Singh and Sharma [22] proposed a new clustering algorithm that employs Particle Swarm Optimization (PSO) to extend network lifetime. The algorithm operates in three phases. In the first phase (cluster formation), the sink node collects each sensor's identifier, location, and current energy level. It then calculates the average node energy and uses PSO to determine the optimal number of CHs that minimizes a defined cost function. The second phase establishes inter-cluster communication paths for data transmission, while the third phase handles the forwarding of aggregated data from CHs to the sink node.

In Ref. [23], the authors presented an Improved Distributed Energy-Efficient Clustering (IDEEC) algorithm for heterogeneous WSNs. The protocol runs in rounds and first evaluates energy consumption to set a minimum threshold per round. It then assesses the residual energy of nodes and selects CHs accordingly. IDEEC also calculates the optimal number of CHs per round using a probability function that favors high-energy nodes while maintaining an ideal CH count.

The authors in Ref. [24] developed a system to detect, identify, and prevent black hole attacks in mobile WSNs. Their approach uses a hierarchical cluster topology with four levels: sensor nodes, cluster heads (CH), coordinator nodes (CO), and base station (BS). Each cluster includes one or more CHs and COs. Sensor nodes collect and send data to CHs, which aggregate it and forward it to COs, and finally to the BS. A trust model is integrated into the detection mechanism, where node behavior is evaluated through packet delivery ratios during neighborhood discovery. Untrustworthy nodes are identified and added to a blacklist for revocation.

In Ref. [25], the authors proposed EPMS, a clustering algorithm based on PSO for improving routing performance. The process begins by dividing the network into regions using PSO. Each node then calculates its distance to the region's center of gravity. The average residual energy of all nodes in the region is computed, and a node is selected as CH if it has above-average remaining energy and is closest to the center of gravity.

The work in Ref. [26] introduced a black-hole detection model for WSN-based Smart Grid applications that relies on a clustering algorithm. CHs are elected based on trust factors calculated from energy levels, honesty, intimacy, and the trade-off between dropped packet ratios. This ensures that only legitimate nodes become CHs.

Fatima et al. [27] aimed to reduce energy consumption and prolong network lifetime by enhancing the weighted clustering algorithm. They incorporated additional parameters into the CH selection process, including inter-node distance, residual energy, and coactivity. The CH election involves comparing the Received Signal Strength Indication (RSSI) against a predefined threshold; nodes with RSSI below the threshold are classified as malicious and excluded from the CH election.

Each non-malicious node calculates a weight based on the selected parameters and broadcasts it. Nodes with the highest weights are elected as CHs, while others join as regular cluster members.

Table 1 presents a comparison of the above clustering algorithms according to various criteria.

Table 1. Comparison of clustering algorithms.

Authors	Routing approach (classical, optimized)	Control manner (Centralized C, distributed D)	Clustering Properties			Heterogeneity	CH s	
			Cluster size (Variable V/Fixed F)	Inter-cluster routing	Intra-cluster routing		Probabilistic	
						Homogeneous/Heterogeneous network	Hybrid Based	Energy Based
Zahedi [19]	Classical	D	V	Single-Hop	Single-Hop	Homogeneous	-	√
Singh and Sharma [22]	Optimized	C	V	Multi-Hop	Single-Hop	Homogeneous	√	-
Xie and Wang [23]	Classical	D	V	Single-Hop	Single-Hop	Heterogeneous	-	√
Pathak et al. [24]	Classical	D	V	Multi-Hop	Single-Hop	Heterogeneous	√	-
Wang et al. [25]	Optimized	C	V	Multi-Hop	Multi-Hop	Homogeneous	-	-
Otoum et al. [26]	Classical	C	V	Single-Hop	Single-Hop	Homogeneous	-	-
Belabed and Bouallegue [27]	Classical	C	F	Single-Hop	Single-Hop	Homogeneous	-	-
Rehman et al. [21]	Classical	D	V	Single-Hop	Single-Hop	Heterogeneous	-	-
Proposed Algorithm	Classical	D	F	Single-Hop	Single-Hop	Homogeneous	-	-

- Cluster Size: Clusters can be formed with either equal or unequal sizes, depending on the number of nodes they contain. In equal-size clustering, all clusters have a predetermined fixed number of members. In unequal-size clustering, cluster sizes vary [27].
- Heterogeneity of the Energy Level: This refers to differences in energy levels among sensor nodes. A two-level heterogeneous WSN includes advanced nodes with higher energy and normal nodes with lower energy [28].

- Heterogeneity: WSNs are categorized as homogeneous or heterogeneous based on variations in sensor node capabilities, such as processing power, storage capacity, and battery power [29].
- CH Selection: Cluster heads can be selected using different strategies, including energy-based, hybrid-based, probabilistic, or non-probabilistic methods.
- Routing Approach: Routing can follow either a classical or an optimized approach. Classical routing relies on timer-based functions for base node selection, often leading to uneven traffic distribution. Optimized routing employs algorithms such as Fuzzy Logic (FL), Genetic Algorithm (GA), or Particle Swarm Optimization (PSO) [28].
- Clustering Control: Clustering can be managed centrally or distributedly. In centralized control, the sink node gathers global network information (e.g., energy levels) and selects the CHs. In distributed control, sensor nodes collaborate locally to form clusters [28].
- Inter-Clustering Routing: Communication between CHs (or sensor nodes) and the sink node can be single-hop (direct) or multi-hop (through intermediate nodes) [28].
- Intra-Clustering Routing: Member nodes can communicate with their CH using either single-hop (direct) or multi-hop (via intermediate nodes) communication [28].

Table 1 compares various clustering algorithms based on the criteria outlined above. The analysis reveals that optimized approaches for CH selection generally provide superior performance in terms of fault tolerance, energy efficiency, and overall robustness, as demonstrated in [25]. For secure clustering, incorporating a trust metric is essential. This metric can be calculated using factors such as packet delivery ratio [23], received signal strength [27], and successful packet reception rate [21]. Additionally, considering residual energy levels is crucial for extending network lifetime, and most reviewed studies include this parameter in CH selection [19, 23, 25, 26].

Most of the discussed protocols rely on single-hop communication for both inter- and intra-cluster routing. Furthermore, nearly all of them produce clusters of variable sizes and adopt centralized control mechanisms [22, 25-27]. However, variable cluster sizes lead to unbalanced workloads on cluster heads. At the same time, centralized approaches struggle with scalability in large-scale SG deployments due to the high number of sensors and extensive coverage areas.

To address these limitations, we propose a new distributed clustering algorithm in which sensor nodes collaborate to form clusters and elect suitable CHs using a hybrid set of parameters. The proposed algorithm creates fixed-size, 1-hop clusters to ensure balanced load distribution among CHs.

Materials and Methods

Overview

Public Key Infrastructure (PKI) offers greater efficiency than shared-key approaches for managing credentials, especially in large-scale networks [9]. In PKI, each device possesses a unique public-private key pair. The Certification Authority (CA) is responsible for issuing, revoking, and updating digital certificates that bind sensor node identities to their public keys. A Registration Authority (RA) authenticates and recommends nodes to the CA.

To overcome the availability and scalability issues associated with a centralized CA in Smart Grid environments, we propose distributing the CA role across multiple sensor nodes, dynamically elected via a clustering algorithm. Each cluster includes one CA (the Cluster Head), at least one RA, and several Member Nodes (MNs). Due to the critical nature of the role, a CH must be highly trustworthy to prevent malicious nodes from being elected. It must also possess the highest energy level among candidates and have at least two trustworthy neighbors. The RA, likewise a trustworthy node,

protects the CA and stands ready to replace it if the CH becomes unavailable. The details of the proposed clustering algorithm are presented in the following section.

Clustering algorithm

The proposed clustering algorithm selects CHs based on multiple parameters. The primary factors include the residual energy level of sensor nodes (to maximize cluster lifetime), the node degree (number of direct neighbors), and a trust metric. A node with fewer than two neighbors cannot become a CH. The trust metric ranges from 0 to 1 and reflects the node's cooperative behavior and the authenticity of messages it transmits. A node is considered fully trustworthy when its trust value reaches 1. Trust values increase through consistent positive behavior and collaboration. Several techniques in the literature compute trust based on packet delivery ratio and Received Signal Strength Indicator (RSSI) [10, 21, 26].

The clustering process consists of three main phases: discovery, clustering, and maintenance.

In the discovery phase, every sensor node exchanges HELLO messages with its one-hop neighbors. These messages contain essential information such as position, current trust metric, and energy level. HELLO messages are broadcast periodically during a predefined period called TimerD.

Once TimerD expires, the algorithm enters the clustering phase. Each node calculates its degree level (DL), which is the number of its neighbors. A trustworthy node with the highest energy level (EL) among its neighbors and at least two neighbors broadcasts an E-message declaring itself a CH candidate. Otherwise, the node waits to receive E-messages from other candidates and sends a join request (J-message) to one of them. The collection of E-messages continues for a duration defined by TimerE.

When TimerE expires, each CH candidate compares itself to the others. If it has the highest energy level (EL) and highest degree level (DL), and it has received at least one join request, it declares itself the CH by broadcasting a HELLO message and accepts all join requests. Otherwise, it joins another CH. All clusters are designed to have a fixed maximum number of member nodes to maintain load balance. **Figure 1** illustrates the flowchart of the proposed clustering algorithm.

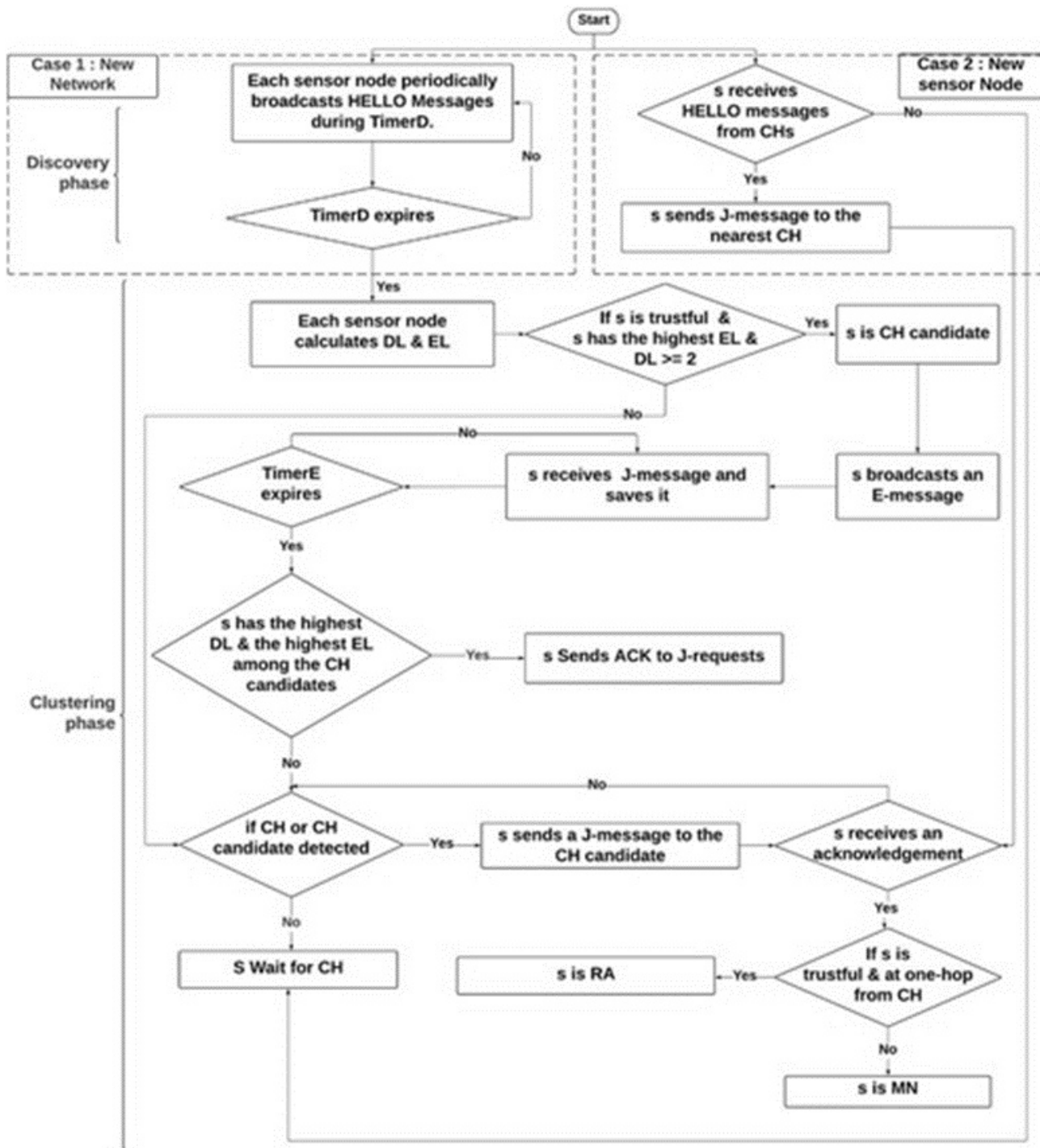


Figure 1. Flowchart of the proposed clustering algorithm.

If a new sensor node enters the network afterward, it listens for HELLO messages from active CHs and sends a join request to the closest one. Should it fail to receive an acknowledgment within the TimerA interval, it attempts to join another CH by sending a new J-message. Once admitted into a cluster, the node's role is assigned according to its trust value and distance: trustworthy nodes located one hop from the CH are designated as Registration Authorities (RAs). In contrast, others function as regular member nodes.

In the maintenance phase, every CH periodically broadcasts HELLO messages to inform its members that it remains active. Simultaneously, RA nodes send their own periodic HELLO messages to the CA. The CA continues operating only as long as it has at least one RA within the cluster. If all RAs are lost, the CH loses its authority, triggering a new clustering cycle.

Characteristics of the proposed PKI

Thanks to the clustering mechanism, the architecture provides a fully distributed, autonomous PKI. Every cluster includes one CA (the CH), one or more RAs, and several ordinary Member Nodes (MNs) with the following responsibilities:

- CA: Serves as the cluster head and handles the issuance and management of short-term certificates for RAs and MNs.
- RA: A reliable node positioned one hop from the CA. It validates MN certification requests and forwards only legitimate ones to the CA. Requests are accepted only when supported by a valid long-term certificate.
- MN: An ordinary sensor node without any special duties inside the cluster.

All sensor nodes are assumed to start with long-term certificates issued offline by a central CA, which helps verify their identity when joining the network. Traditional PKI systems require frequent contact with a central CA to renew certificates and avoid spoofing. However, in large SG deployments — characterized by vast areas, high node counts, and unstable links — such repeated long-distance communication is impractical and can leave nodes unable to participate.

The proposed design solves this by letting each node obtain a short-term certificate from its local CH for intra-cluster communication. When a short-term certificate expires, or a node is suspected of compromise, it simply contacts its CH. Using the node's long-term certificate for authentication, the CH issues a locally generated short-term certificate. This greatly reduces renewal latency and enables fast revocation of compromised keys without depending on a distant central authority.

Overall, this distributed PKI overcomes key weaknesses of centralized systems. It removes the single point of failure by spreading CA duties across dynamically elected nodes selected based on topology and multiple criteria. A compromise or failure of one CA affects only its own cluster. RAs add extra protection by screening requests and defending against DoS attacks. Trust-based clustering prevents malicious nodes from becoming CAs. Asymmetric cryptography delivers strong authentication, confidentiality, and non-repudiation. Short-term certificates further reduce the risks of sinkhole and Sybil attacks through regular local key renewal.

Results and Discussion

This section assesses the scalability and overall performance of the proposed clustering algorithm.

Simulation setup

The experiments were carried out using the OMNET++ network simulator, which uses C++ modules interconnected through message exchange [30]. The clustering algorithm was developed and tested inside the Castalia simulator [31], a well-established platform for evaluating WSN protocols before hardware implementation.

The performance evaluation involved a network of approximately 200 nodes arranged in a grid across a 100 × 100 meter area. The detailed simulation parameters are provided in [Table 2](#).

Table 2. The simulation parameters.

Parameters	Values
The number of sensor nodes	200
Network size	100 × 100 m
Max number of nodes in a cluster	25
Percentage of malicious sensor nodes	(5, 25)
Simulation duration	2000 s

Simulation results

We first analyze the number of elected Certification Authorities (CAs). As shown in [Figure 2](#), the number of CAs is plotted against the total number of nodes in the network.

The figure reveals a clear trend: as the network size grows, the number of elected CAs rises accordingly. Specifically, for a network of 150 nodes with a cluster size limit of 30 members, 5 CAs are elected. This number increases to 6 CAs when the network expands to 200 nodes.

All clusters maintain a fixed capacity equal to the maximum number of allowed members. Whenever a cluster becomes full, an additional cluster is automatically formed. [Figure 2](#) further highlights that increasing the maximum cluster size results in fewer CAs overall.

These outcomes demonstrate that the proposed clustering algorithm effectively minimizes the number of CAs while ensuring every node can join a cluster. New clusters are established only when existing ones reach their capacity.

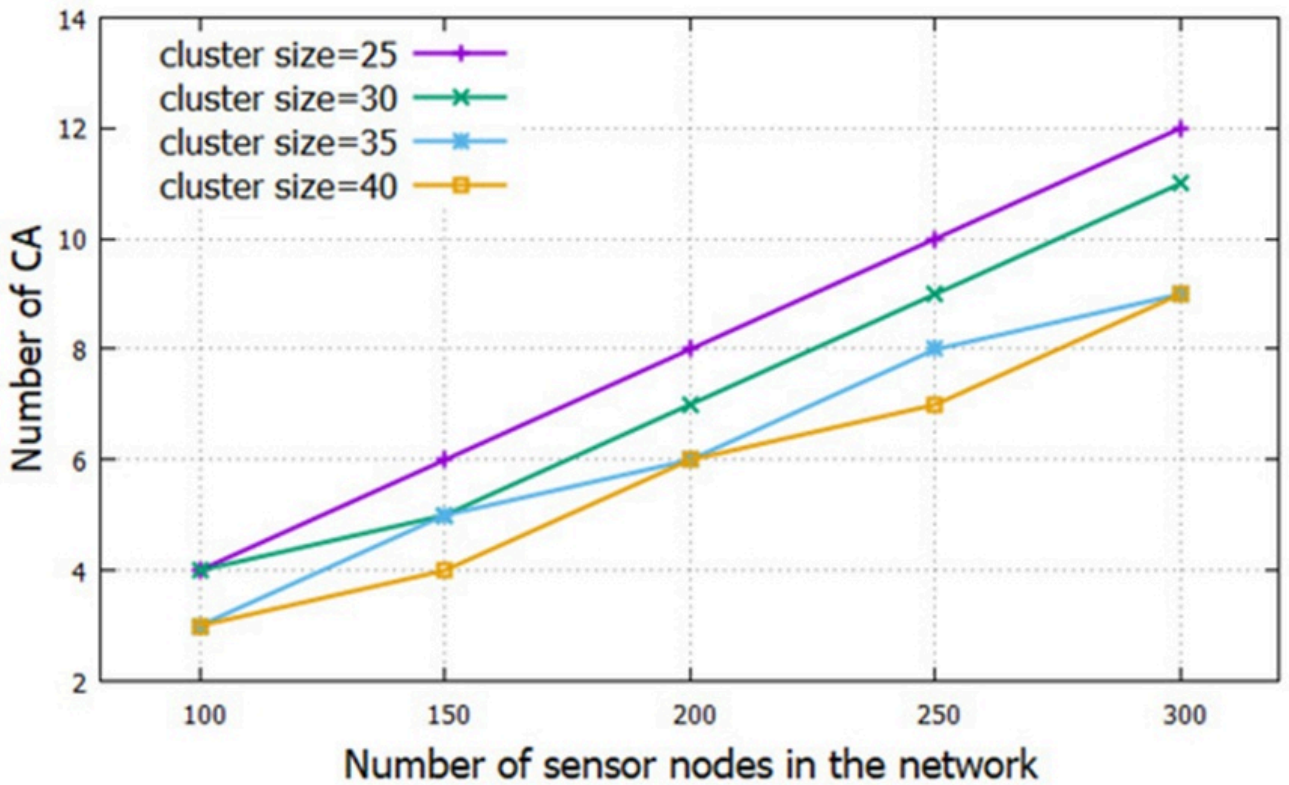


Figure 2. Number of elected CAs per total number of sensor nodes in the network.

Figure 3 demonstrates how the transmission range influences the number of selected CAs. Given that the algorithm targets Smart Grid settings with a large number of widely scattered sensors across extensive sites, the simulations employed relatively large transmission ranges exceeding 50 meters.

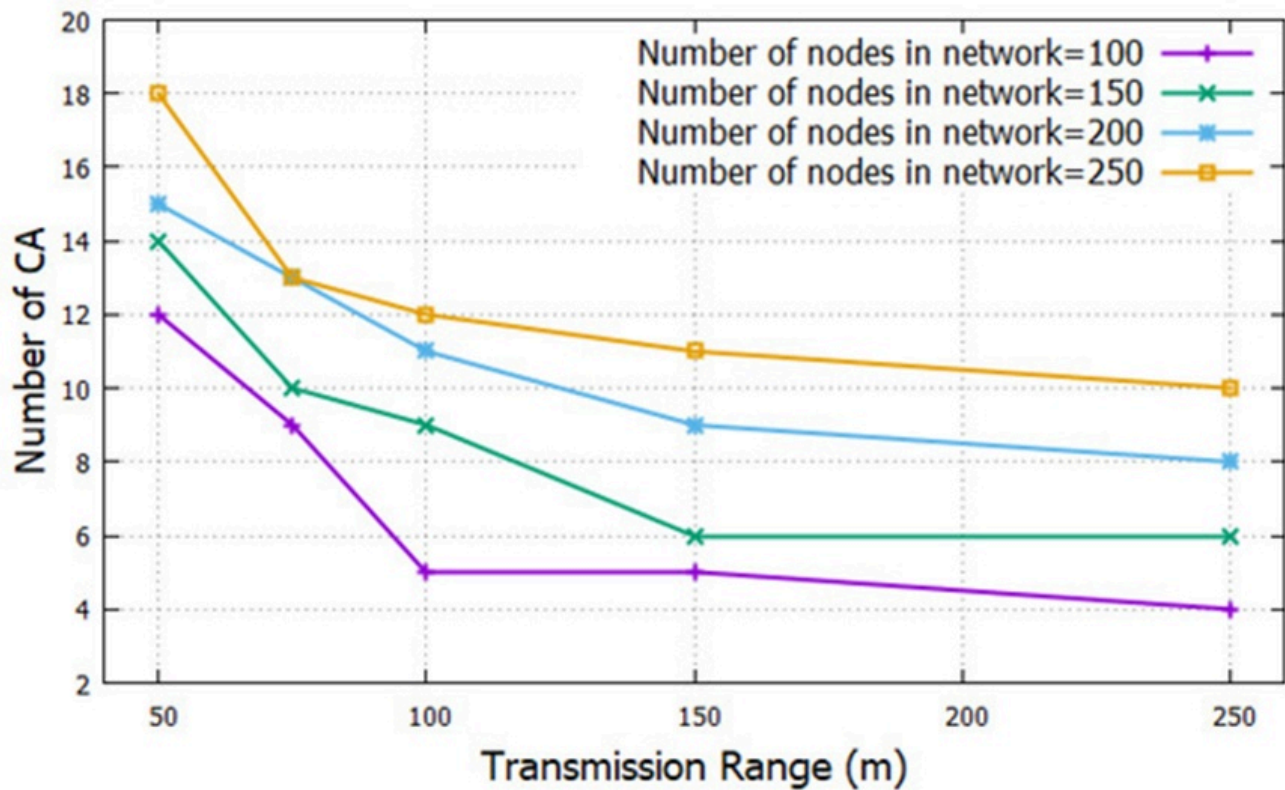


Figure 3. Number of elected CAs as a function of transmission range.

As displayed in **Figure 3**, the number of CAs drops noticeably when the transmission range becomes larger. For a network of 250 sensor nodes with a cluster size of 25, the system creates 18 clusters at a 50 m range, but this number falls sharply to just 10 clusters when the transmission range reaches 250 m.

The reason is simple: with greater transmission ranges, distant nodes can reach existing CHs more easily. This leads to fewer cluster heads being selected and, therefore, fewer clusters being formed. It is important to note that larger transmission ranges consume more energy, which is why the maximum value was capped at 250 m in these experiments.

Figure 4 shows that the number of elected CAs remains completely stable regardless of the number of malicious nodes in the network. This robustness comes from two main protections built into the design. First, the CH selection process relies heavily on a trust metric, so malicious nodes have no chance of being elected as CAs. Second, the Registration Authority carefully filters all incoming join requests, preventing any malicious attempts from reaching or compromising the CA.

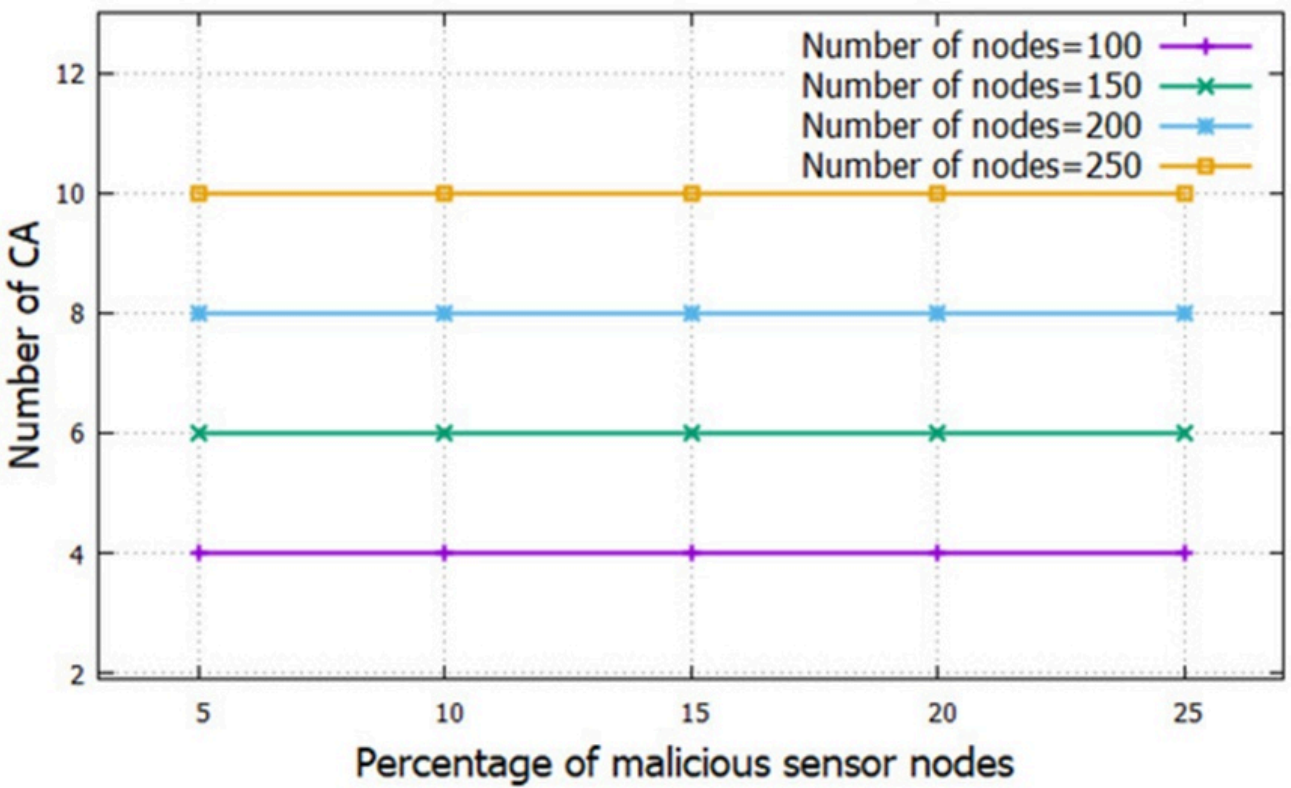


Figure 4. Variation in the total number of cluster heads (CAs) according to the proportion of malicious sensor nodes present in the network.

Figure 5 compares the rate at which malicious sensor nodes are selected as cluster heads (CAs) relative to the overall number of malicious nodes. Results are shown for the suggested method and for the Energy Efficient Secure trust-based (EEST) clustering approach [20] from the literature review. The graph shows that approximately 10% of malicious nodes are elected as CAs when using EEST, whereas the proposed method prevents any malicious nodes from becoming CAs. This strong security property stems from the incorporation of a trust evaluation mechanism during the selection process, ensuring that only highly trustworthy sensor nodes are eligible to serve as CAs.

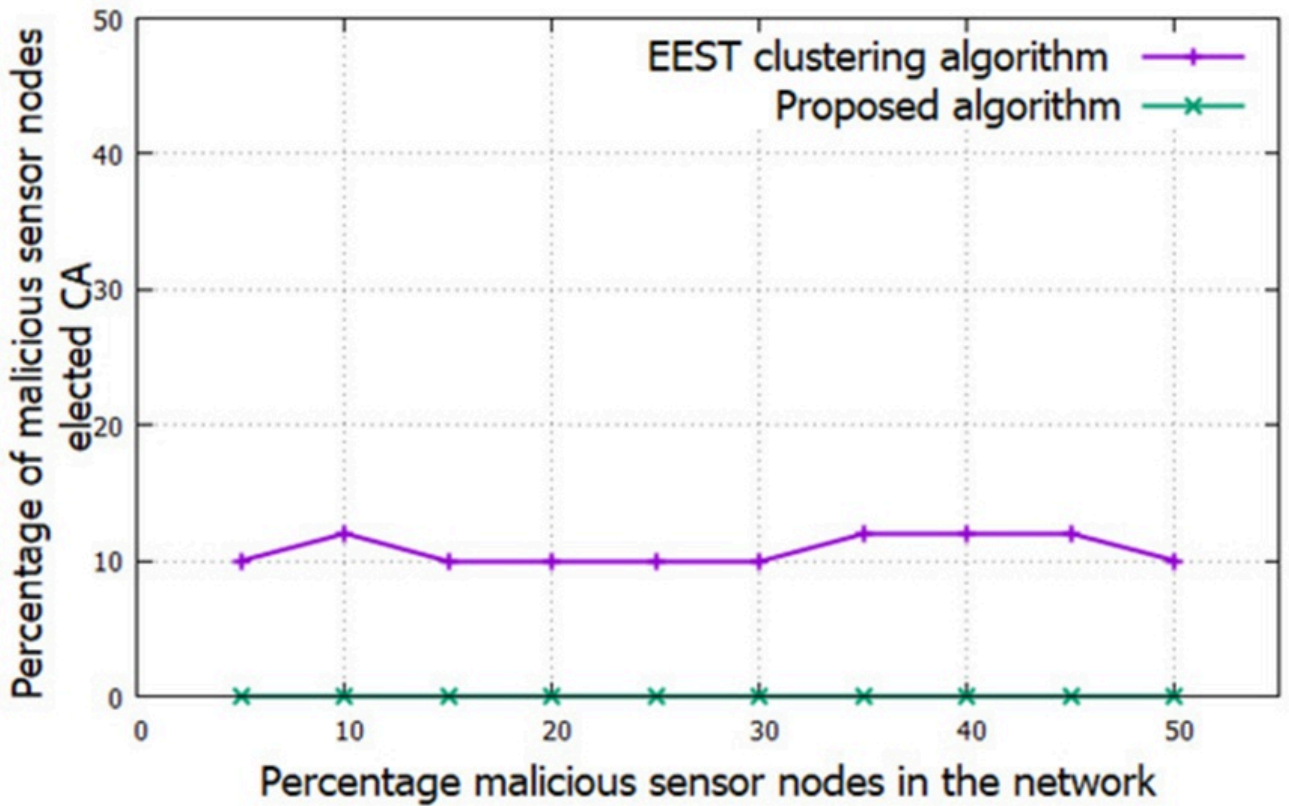


Figure 5. Ratio of malicious sensor nodes chosen as cluster heads (CAs) plotted against the overall number of malicious nodes present in the network.

Figure 6 displays the share of sensor nodes successfully integrated into clusters relative to the total number of deployed sensor nodes. At a transmission range of 100 m, roughly 2% of nodes remain outside any cluster. This situation arises mainly when nodes have restricted communication distance or are positioned at the outer boundaries of the deployment field, making it impossible for them to associate with an existing CA. Additionally, malicious nodes are barred from establishing their own clusters. In contrast, at greater transmission ranges, the figure demonstrates that all sensor nodes (100%) are incorporated as cluster members. These findings highlight the robustness and effectiveness of the proposed clustering approach, demonstrating that the resulting clusters achieve complete network coverage.

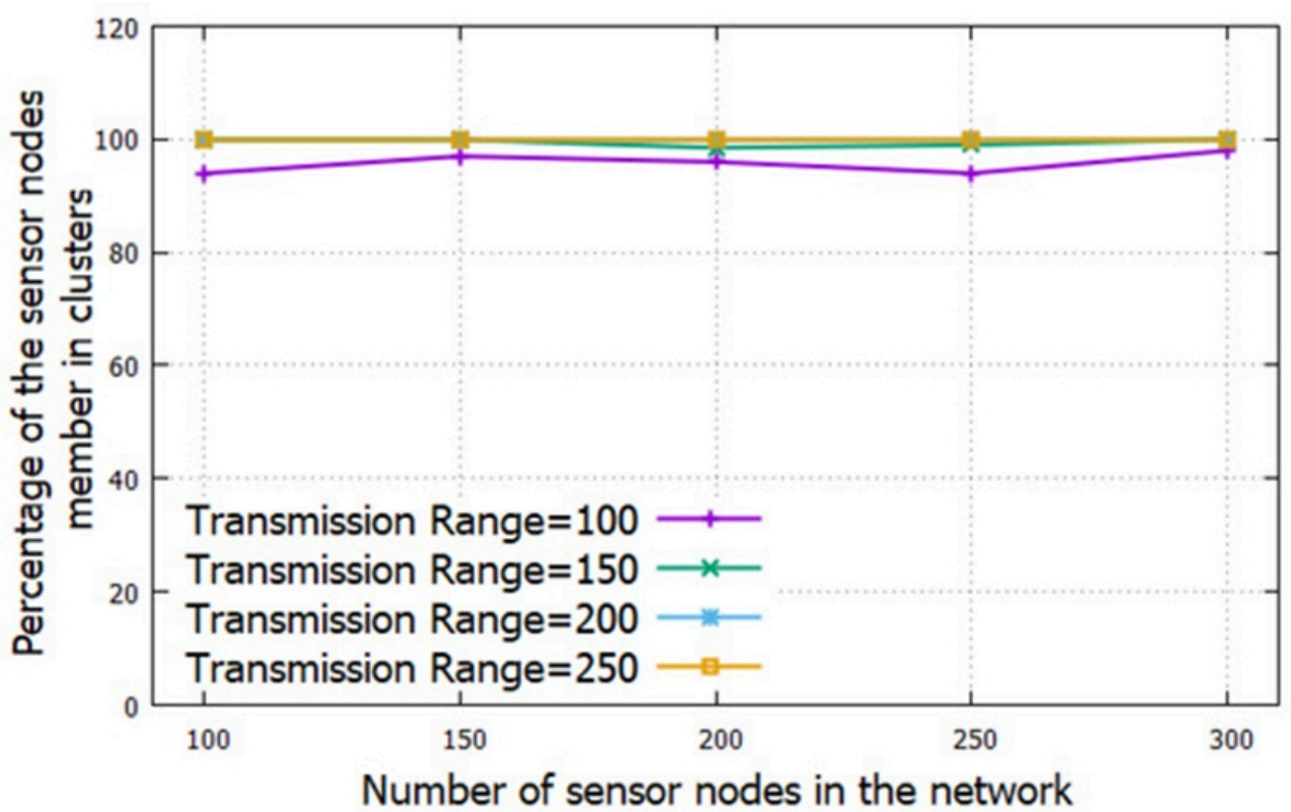


Figure 6. The proportion of sensor nodes in clusters, plotted against the total number of nodes in the network.

Figure 7 shows the network's energy consumption as the number of sensor nodes increases. The results reveal that Cluster Heads (CHs) consume only marginally more energy compared to regular sensor nodes. This suggests that the additional responsibilities of a CH — such as periodically broadcasting HELLO messages and handling join acknowledgments — do not impose a substantial energy burden. At the same time, overall energy consumption increases as the network size grows, primarily because more HELLO and control messages are exchanged during cluster formation. However, even in larger networks, the total energy used stays minimal, remaining well below 1% of each sensor node's initial energy reserve.

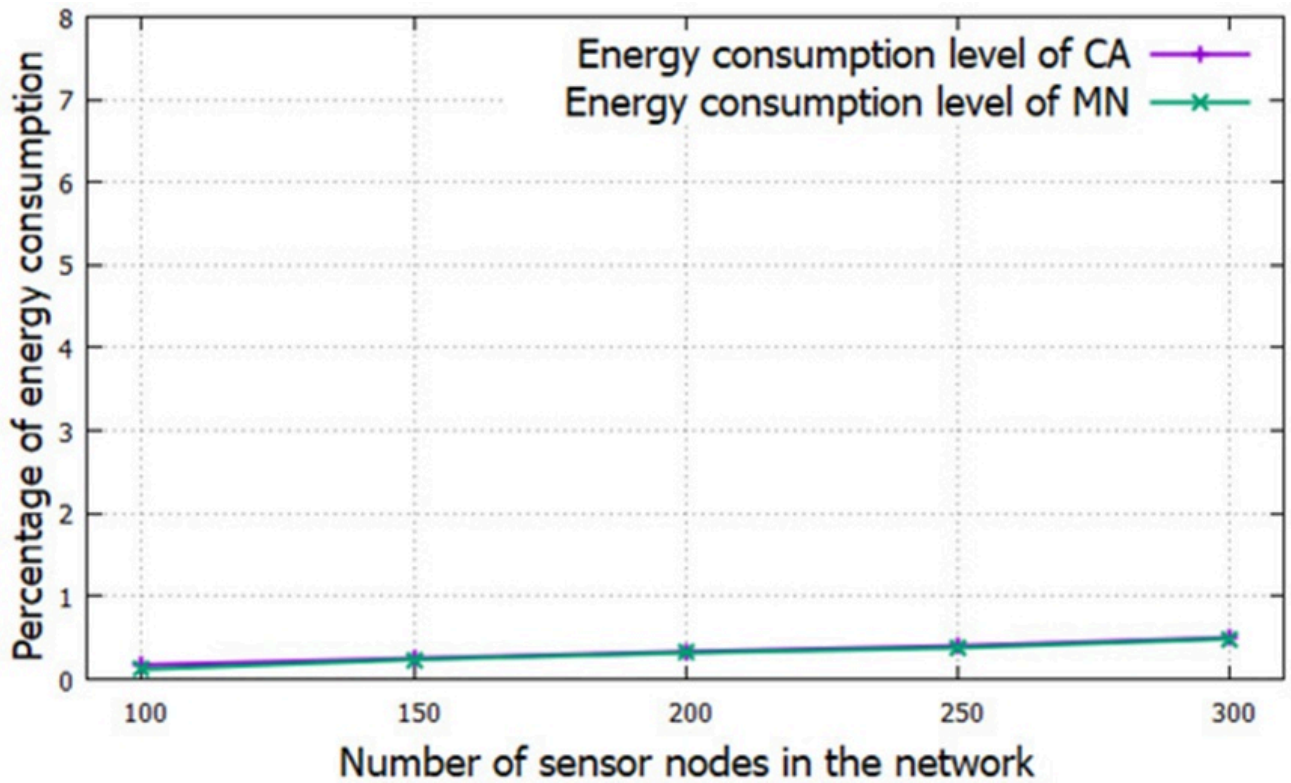


Figure 7. Energy consumption percentage relative to the total number of sensor nodes in the network.

In **Figure 8**, the cluster head lifetime is plotted against the percentage of malicious nodes in the network. The cluster head (CA) achieves 100% lifetime, remaining active throughout the network's operation. This strong performance stems from the requirement to have at least one Registration Authority (RA) within the cluster and sufficient remaining energy. These outcomes demonstrate the high stability of the proposed clustering approach, in which sensor nodes seldom need to leave or change their current cluster.

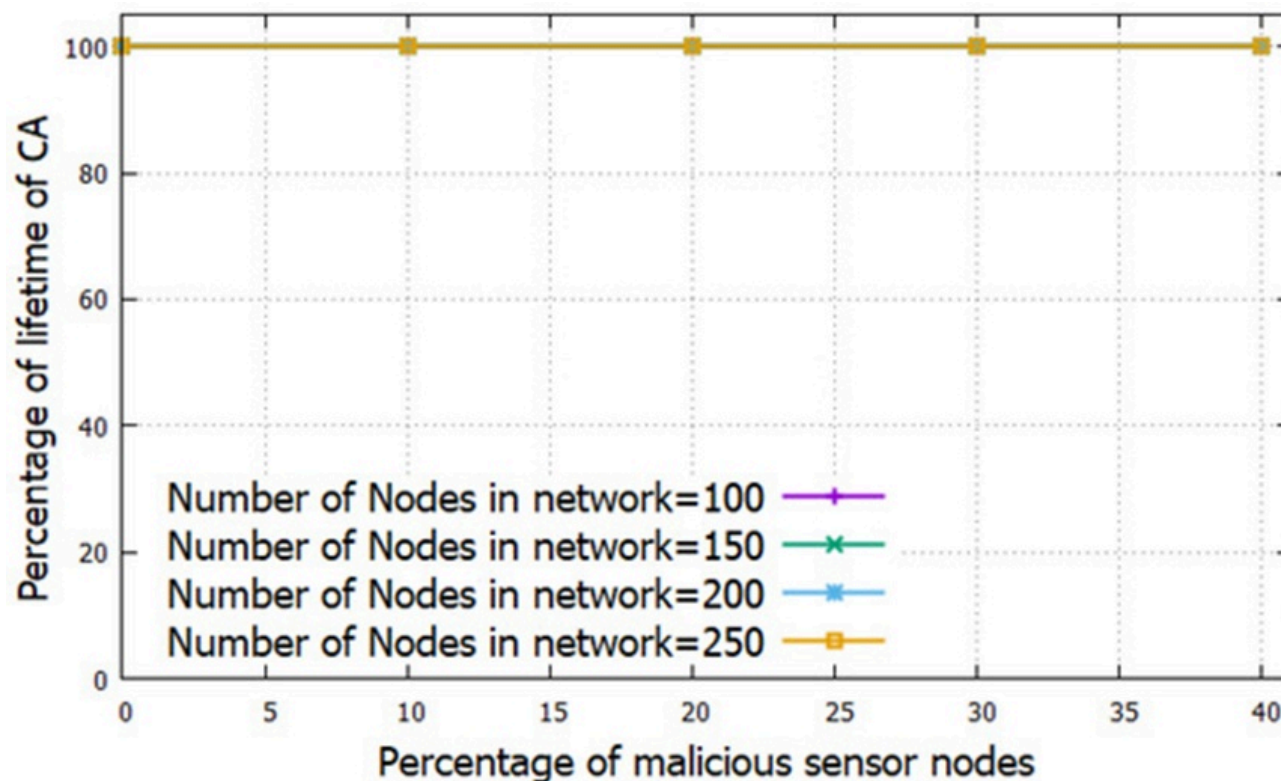


Figure 8. The lifetime of the CA as a function of the percentage of malicious sensor nodes.

Conclusion

This study presents an innovative security framework for WSNs in SG environments, employing a distributed PKI in which the responsibilities of a centralized CA are distributed to dynamically elected sensor nodes via a clustering approach. The main goal is to prolong CA service availability and eliminate the vulnerability of a single point of failure. The election process uses a trust-based metric to evaluate sensor node behavior, ensuring that any compromise of a CA affects only its own cluster. Simulation results show that nearly all nodes are effectively clustered and that the selected CAs maintain a long operational lifespan, confirming the robustness of the distributed PKI. Additionally, the architecture scales efficiently: as the network grows, new clusters form automatically, preventing overload or denial-of-service on existing CAs. On the security front, the framework enables secure node-to-node communications; possession of valid certificates and keys mitigates Sybil attacks, while encryption protects against eavesdropping.

For future development, we plan to implement a comprehensive trust management system for SG-based WSNs to continuously evaluate and maintain node trust levels, alongside enhancements to PKI operations, particularly certificate issuance and revocation procedures.

Acknowledgements

None

Conflict of interest

None

Financial support

This research was funded by the University of Jeddah, Saudi Arabia, grant number UJ-20-124-DR

Ethics statement

None

Received: 29 Mar 2025

Revised: 10 May 2025

Accepted: 20 Jun 2025

Published online: 20 September 2025

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Rekik S, Baccour N, Jamiel M, Drira K. Wireless sensor network based smart grid communications: Challenges, protocol optimizations, and validation platforms. *Wirel Pers Commun*. 2017;95:4025-47.
- Tuna G, Örenbaş H, Daş R, Kogias D, Baykara M, Gülez K. Information security threats and an easy-to-implement attack detection framework for wireless sensor network-based smart grid applications. In: *Proceedings of the 5th International Conference on Materials and Applications for Sensors and Transducers*; 2015 Sep 27-30; Mykonos, Greece.
- Mehmood G, Khan MS, Waheed A, Zareei M, Fayaz M, Sadad T, et al. An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network. *Complexity*. 2021;2021:6577492.
- Amutha J, Sharma S, Sharma SK. Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. *Comput Sci Rev*. 2021;40:100376.
- Chhaya L, Sharma P, Bhagwatikar G, Kumar A. Wireless sensor network based smart grid communications: Cyberattacks, intrusion detection system and topology control. *Electronics*. 2017;6(1):5.
- Liu Y. Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenges. *Int J Distrib Sens Netw*. 2012;8:1-8.
- Alfandi O, Bochem A, Kellner A, Hogrefe D. Simple secure PKI-based scheme for wireless sensor networks. In: *Proceedings of the 2011 Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing*; 2011 Dec 6-9; Adelaide, Australia. p. 359-64.
- Nandhini M, Praveenkumar B. An Implementation of Public Key Infrastructure Using Wireless Communication Networks. *Int J Grid Distrib Comput*. 2015;8:35-42.
- Mahmoud MMEA, Mišić J, Shen X. A scalable public key infrastructure for smart grid communications. In: *Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM)*; 2013 Dec 9-13; Atlanta, GA, USA. p. 784-9.

He D, Chan S, Zhang Y, Guizani M, Chen C, Bu J. An enhanced public key infrastructure to secure smart grid wireless communication networks. *IEEE Netw*. 2014;28(1):10-6.

Shahzad F, Pasha M, Ahmad A. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. *IJCSIS*. 2017;14:54-65.

Kivande MV, Wade AM. Adaptive and Channel Aware Forwarding Attack Detection for Mobile Sensor in WSN with Security of Data. *Int J Eng Sci*. 2017;7:13256.

Riaz MN. Clustering algorithms of wireless sensor networks: A survey. *Int J Wirel Microw Technol*. 2018;8:40-53.

Rostami AS, Badkoobe M, Mohanna F, Keshavarz H, Hosseinabadi AAR, Sangaiah AK. Survey on clustering in heterogeneous and homogeneous wireless sensor networks. *J Supercomput*. 2018;74:277-323.

Fanian F, Rafsanjani MK. Cluster-based routing protocols in wireless sensor networks: A survey based on methodology. *J Netw Comput Appl*. 2019;142:111-42.

Arjunan S, Sujatha P. A survey on unequal clustering protocols in Wireless Sensor Networks. *J King Saud Univ - Comput Inf Sci*. 2019;31:304-17.

Zeb A, Islam AKMM, Zareei M, Al Mamoon I, Mansoor N, Baharun S, et al. Clustering Analysis in Wireless Sensor Networks: The Ambit of Performance Metrics and Schemes Taxonomy. *Int J Distrib Sens Netw*. 2016;12:1-12.

El Khediri S. Wireless sensor networks: A survey, categorization, main issues, and future orientations for clustering protocols. *Computing*. 2022;104:1-63.

Zahedi A. An efficient clustering method using weighting coefficients in homogeneous wireless sensor networks. *Alex Eng J*. 2018;57:695-710.

Koucheryavy A, Salim A. Cluster head selection for homogeneous Wireless Sensor Networks. In: *Proceedings of the 2009 11th International Conference on Advanced Communication Technology*; 2009 Feb 15-18; Gangwon, Korea.

Rehman E, Sher M, Naqvi SHA, Khan KB, Ullah K. Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network. *J Comput Netw Commun*. 2017;2017:1630673.

Singh SP, Sharma SC. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI—2018)*. In: Springer International Publishing; 2020; Madurai, India. p. 1775-80.

Xie B, Wang C. An improved distributed energy efficient clustering algorithm for heterogeneous WSNs. In: *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC)*; 2017 Mar 19-22; San Francisco, CA, USA.

Pathak GR, Patil SH, Tryambake JS. Efficient and trust based black hole attack detection and prevention in WSN. *Int J Comput Sci Bus Inform*. 2014;14:93-103.

Wang J, Cao Y, Li B, Kim HJ, Lee S. Particle swarm optimization based clustering algorithm with mobile sink for WSNs. *Futur Gener Comput Syst*. 2017;76:452-7.

Otoun S, Kantarci B, Mouftah HT. Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring. In: *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*; 2017 May 21-25; Paris, France.

Belabed F, Bouallegue R. An optimized weight-based clustering algorithm in wireless sensor networks. In: *Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*; 2016 Sep 5-9; Paphos, Cyprus. p. 757-62.

Sabor N, Sasaki S, Abo-Zahhad M, Ahmed S. A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions. *Wirel Commun Mob Comput*. 2017;2017:2818542.

Velmurugan S, Logashanmugham E. Secure Mobile Beacon Based Obstacle Awareness in WSN. *IIOAB J*. 2017;8:1-7.

Varga A. Using the OMNeT++ discrete event simulation system in education. *IEEE Trans Educ*. 1999;42:11.

Castalia User Manual [Internet]. [cited 2021 Oct 25]. Available from: <http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/INGRES-M1/Castalia%20-%20User%20Manual.pdf>