smart cities

MDPI

Article

A Novel Security Architecture for WSN-Based Applications in Smart Grid

Nouf Aljadani and Tahani Gazdar *

College of Computer Science and Engineering, University of Jeddah, Jeddah 23447, Saudi Arabia; naljadani.stu@uj.edu.sa
* Correspondence: taalgazdar@uj.edu.sa

Abstract: The Smart Grid (SG) aims to cope with the problems of the traditional grid, using renewable power generators. Similarly, SG benefits from the deployment of wireless sensor networks (WSNs) to enhance its aspects by monitoring the physical behavior of the power generators. However, new threats and attacks may arise due to the open nature and large scale of SG where WSNs are deployed. In this paper, we propose a new security architecture for WSNs in SG based on public key infrastructure (PKI). The key idea of the proposed architecture is to distribute the role of the certification authority (CA) among a set of sensor nodes to ensure the availability and scalability of the CA services. To elect this set of sensor nodes, we propose a novel lightweight clustering algorithm for WSNs that relies on the trust metrics of the nodes and their energy levels. The proposed architecture provides many security services such as authentication and confidentiality and mitigates many types of attacks such as Sybil and eavesdropping. Extensive simulations have been conducted using network simulator OMNET++ and Castalia framework to investigate the performance of the clustering algorithm. The results show that almost 100% of the sensors are members of clusters, and even in the presence of malicious nodes, the number of cluster heads remains static which reflects the robustness of the proposed architecture.

Keywords: Smart Grid (SG); wireless sensor networks (WSNs); public key infrastructure (PKI); clustering; certification authority (CA)

check for updates

Citation: Aljadani, N.; Gazdar, T. A Novel Security Architecture for WSN-Based Applications in Smart Grid. *Smart Cities* **2022**, *5*, 633–649. https://doi.org/10.3390/smartcities5020033

Academic Editor: Pierluigi Siano

Received: 2 April 2022
Accepted: 6 May 2022
Published: 10 May 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

1.1. Background

In recent decades, the protection of the environment made governments throughout the world change the existing electrical grid to a smart electrical grid. The regeneration of a traditional electric grid is needed based on many weaknesses. Particularly, the traditional power grid uses nonrenewable power resources which leads to gas emissions and climate changes. Additionally, to control the outage of power, a high amount of unused energy and energy that cannot be stored is produced and consequently wasted. In addition, the traditional electric grid lacks advanced communication techniques and monitoring [1]. SG seeks to improve the efficiency, flexibility, and reliability of the traditional electric grid [2]. The key feature of SG is the use of renewable energy generators like photovoltaic power systems (PPS). The PPS may be deployed on the roof of buildings or the ground, such as solar farms. More importantly, SG is based on a set of different communication technologies that range from wired to wireless technology. It allows the components of the grid, such as generators and substations, to communicate to exchange different types of data considering the following requirements: latency, reliability, bandwidth, security and privacy, scalability, and interoperability. The installation of the energy generators in harsh and open environments arises many problems in the maintenance of the infrastructure and the real-time monitoring of the grid components became more difficult. The energy generators are facing many risks, such as fires leading to burned panels, ice, electric shock,

etc. In this context, WSNs are a promising solution that can be deployed in the case of serious and complex situations where manual operations cannot be applied. The major tasks of WSNs are target tracking and monitoring [3]. WSNs applications allow sharing of information, such as humidity, voltage, and ambient temperature, that helps in real-time monitoring to observe the physical processes and detect problems. Compared with traditional wireless communication, they are characterized by easy deployment, low cost, and large area coverage [4].

1.2. Problem Statement

The result of different communication technologies in the SG is a potential increase in the security risk. Apart from that, the security of WSNs-based applications in SG needs attention for many reasons. The open nature of WSNs makes them vulnerable to different attacks, such as the Denial of Service (DoS), selective forwarding, sinkhole, and Sybil [5]. Furthermore, WSNs are deployed in large solar and wind farms. Additionally, many research efforts interested in the security of WSNs-based applications in SG focus more on the consumer side. The power generation side is broadly neglected. However, the existence of internal or external attacks on WSNs should not affect the availability of the SG services and the energy generation. Hence, security is a critical problem in WSNs applications and many security requirements should be considered. Non-repudiation is one of the important requirements, it prevents sensor nodes from denying their actions and messages. Integrity is another requirement; it ensures that the transmitted data are not altered by an illegitimate entity [5]. The authentication validates that the identity of the sensor node that sent a message is what it claimed. Additionally, confidentiality protects sensitive data from being disclosed [6]. Distinct efforts have been made to design security schemes for WSNs in SG. The existing schemes are categorized as encryption-based and non-encryption-based solutions, and this depends on the nature of the threats. Non-encryption-based solutions target only some types of attacks and provide only some security requirements. However, the encryption-based solutions mitigate a larger set of attacks and ensure many security services, such as confidentiality and integrity. PKI is a potential mechanism that provides the most security requirements for WSNs in SG [5]. The authentication and the non-repudiation can be satisfied by a digital signature, the integrity is ensured using a keyed hash function and confidentiality is guaranteed using encryption [6]. However, PKI has some limitations, particularly the availability and the scalability of the CA due to its centralized architecture. The CA represents a single point of failure, once the CA is compromised, the WSNs will be compromised as well. The compromise of the CA will affect the availability of the certification services in the network. Furthermore, the CA should be able to serve a high number of sensors at the same time and keep the same robustness, independently of the size of the network.

1.3. Contribution

To cope with the aforementioned limitations of centralized PKI, we propose in this research work a new distributed PKI for WSN-based applications in SG. The proposed distributed PKI is built on a clustering algorithm, where the cluster heads (CHs) will play the role of the CA in the clusters. We aim to improve the scalability of the PKI and enhance the availability of the certification process by delegating the role of the CA among CHs. So far, a large number of schemes have been put forward for PKI in WSNs. Two main approaches are adopted in the existing architectures: either the CA or trust authority is a centralized and permanent authority like in [7,8] or the role of the CA is distributed among a set of authorities nominated and preconfigured offline such as in [9,10]. Unfortunately, both approaches suffer from the single point of failure. In the perspective of avoiding this risk and improving the scalability and availability of the CA, in the proposed architecture, its role is delegated to a set of sensor nodes elected dynamically in the network, in so doing, if one CA is compromised, only its cluster will be affected, consequently, the single point of failure is solved. Furthermore, the election of the sensor nodes that will play the role of CA

is achieved using a clustering algorithm. That is why, in this research work, we propose a new clustering algorithm for WSNs deployed in SG. It is based on many parameters, such as the energy level of the sensor nodes, the number of trustful neighbors, and the trust metric of the sensor nodes. A new clustering algorithm is proposed for many reasons. First, the large scale of WSNs in SG requires a lightweight and fast clustering process that does not require an excessive exchange of control messages to save the resources of the sensor nodes. Secondly, almost all clustering algorithms are based only on the location or the energy level, however, these two parameters are not sufficient to elect trustful CHs and balanced clusters. Additionally, since, in the proposed architecture, the cluster head will play the role of the certification authority in its cluster, this requires a high level of trustworthiness. That is why a trust metric is considered in the election process in addition to many others metrics like the energy level and the number of trustful neighbors. The latter will help in maintaining the stability of the architecture. If the CA is lost for any reason (compromise, energy, . . .), its trustful neighbor will replace it. Furthermore, we aim to create balanced clusters to balance the load on the elected cluster heads. Although plenty of clustering algorithms exist in the literature, they provide a great many brilliant ideas but unfortunately, we did not find an algorithm that has all the aforementioned features. The key contribution of this article is summarized as follows:

- A novel clustering algorithm is proposed to elect the CHs. Given the sensitivity of their role, many metrics are considered in the election process, particularly the trust metric of the sensor nodes and the number of trust neighbors. To balance the load on the CHs, the size of the cluster is also considered.
- Then, a distributed PKI is designed where the CHs play the role of the certification authority in their clusters. In each cluster, a registration authority (RA) is responsible for checking the authenticity of the sensor nodes before being certified.
- Afterward, the performance of the clustering algorithm and the robustness of the architecture is evaluated using simulation.

The rest of the paper is organized as follows. In Section 2, we discuss the related work interested in security in WSN-based applications in SG. In Section 3, the related work of clustering protocols in WSNs is reviewed, also a comprehensive classification of the discussed approaches is presented. Section 4 proposes a new distributed PKI based on a clustering algorithm to address the limitations of the existing solutions. The simulation results are presented in Section 5. Section 6 concludes the paper and presents some future works.

2. Security in WSN-Based SG

2.1. Attacks

WSNs suffer from many types of attacks on various network layers [11]. The current work focus on the following four types:

- DoS

Due to the WSNs' limited computational power and capacity of memory, it is vulnerable to Dos attack. Where the network resources will be unavailable. In the context of the PKI, a DoS attack could be conducted against the certification authority which may lead to the failure of the certification process [5].

- Sinkhole Attack

The attacker either brings a fake node in the sensor network or gets an agreement of a real sensor node. The attack occurs when a fake node captures the traffic of the network. Once the attack is successful, the fake node can perform a variety of malfunctions, including deleting or altering data. To avoid this kind of attack a strong authentication mechanism is required [5].

- Sybil Attack

To execute this attack, the malicious sensor node occupies several identities. One of most major goals of this attack is to disorder the routing process and communication in WSNs. This scenario may be avoided using a strong identity management mechanism [5].

- Traffic analysis Attack

To perform this attack, the adversaries analyze the traffic pattern by eavesdropping on wireless communication. Additionally, the adversaries could acquire a lot of information about the network topology and infer the location of important nodes by watching traffic volume and pattern, then launch an active attack, such as DoS. A strong asymmetric encryption scheme could be the first line of defense against eavesdropping [11].

2.2. Related Work

The security solutions for WSN-based application in the SG has been extensively studied recently. The authors in [2] proposed a framework to detect DoS attacks and prevent the direction of the attack to the sink node. The proposed framework blocks suspicious nodes that may cause a DoS attack. If the difference between the current node's request time and its last request time is less than a predefined threshold the node is blocked. Furthermore, the access information of the blocked node is stored, and with each request it sends, the number of requests is incremented. Hence, the suspicious nodes are detected through the number of requests. The limitation in this work is the fact that it is unreasonable to block the node because it may send two or three requests in less time than the predefined threshold. The authors in [12] proposed an adaptive and channel-aware forwarding attack-detection system to detect selective forwarding attacks in WSNs. The authors proposed to divide the network lifetime into a series of evaluation periods and estimate the normal packet loss ratio for every evaluation period to assess the forwarding behavior. In the first phase, the normal packet loss ratio is estimated for all sensor nodes, where the loss of a packet is affected by radio link quality. In the second phase, the sensor nodes monitor their neighbors to evaluate a reputation score periodically. In the third phase, each sensor node computes the probability of attack for its neighbors then it broadcasts the score. The limitation in this work is the use of a non-encryption-based technique which does not satisfy the required security services in the context of WSNs and SG.

Alfandi et al. [7] proposed a scheme based on the hybrid cryptography approach employing public-key cryptography to provide confidentiality and integrity in the transmission of data between sensor nodes. In their scheme, a central CA signs the public key and the network address of each sensor node and redistributes the key, address, and signature. The keys exchange is initiated during a handshake based on certificates. The result of this handshake is two keys generated to be used in symmetric encryption. The limitation of this work is that the central CA represents a single point of failure. Nandini and Praveenkumar [8] proposed to implement a PKI for the SG using wireless communication networks. In the registration process, the binding of the users' entity with a public key is established using the digital signature. A RA ensures the rightness of the binding after the registration process and the CA issues the certificate to the users. Secure communication with a resource starts with a certificate-signing request (CSR) sent to the RA. The validation authority gives the status of the certificate to a relying party (RP) to access secure resources. In this approach, the centralized CA also represents a single point of failure. The authors in [9] proposed a hierarchical PKI for SG. The proposed PKI consists of five levels. The first level named the master level is the base of trust in the system. Its role is to issue the certificate to the next level, its public key is known by all devices, also all devices can communicate with it. Levels two, three, and four have less validity than the first level. Each level issues a certificate to the next level. As we descend in the hierarchy, the responsibility of level narrows to a smaller area. The last level has no validity to issue the certificates, it can just communicate with other devices. The shortcoming of this work is the fact that the master level is considered the base of trust in the system which makes it a single point of failure. The authors in [10] aim to improve an existing PKI in a SG environment. They propose to divide the SG into groups based on the hierarchical communication network

to distribute the trust authority (TA) among the groups to deal with the single point of failure problem.

In a WSN deployed in a Smart Grid. The PKI should keep the same robustness, independently of the number of sensor nodes and the network dimensions. In this paper, we will design a new distributed PKI in WSNs-based applications in SG based on a clustering algorithm to elect a set of sensor nodes eligible to play the role of the CA in their clusters. The election depends on the topology of the network and many other parameters, to ensure the stability and the scalability of the distributed PKI. In the following section, we will review some clustering algorithms in WSNs.

3. Clustering Protocols in WSNs

3.1. Classification of Clustering Protocols in WSNs

The clustering protocols in WSNs may be classified in multiple various ways and based on several parameters [13,14]. Many researchers have contributed to the development of clustering algorithms in WSNs during the past years. In [13], the authors classified the clustering algorithms into two categories: probabilistic algorithms and non-probabilistic algorithms. The authors in [15] classify the cluster-based routing protocols in WSNs into two main classes based on the parameters used in the clustering process: macro parameters and micro parameters. The authors in [16] classify the clustering algorithms into three main categories: probabilistic, deterministic, and preset. In [17], the authors categorized the clustering algorithms in WSNs into seven categories: connected dominated set-based, mobility aware, energy-efficient, load balancing, dynamic, and homogenous/heterogeneous. In [18], the authors classify the clustering algorithms in WSNs into four classes: clustering algorithms for homogenous nodes, clustering algorithms for heterogeneous nodes, clustering algorithms based on fuzzy logic methods, and clustering algorithms based on heuristic methods. In this section, we propose a new comprehensive classification for the clustering algorithms in WSNs based on many criteria as follows:

- Probabilistic/non-probabilistic clustering: each sensor node is assigned with a probability used as the main parameter to select the cluster head nodes [13,19]. In non-probabilistic clustering, many of the basic and specific factors such as the location of the nodes, the number of neighbors, and security factors [20] are considered in the election process of CHs [13].
- Clustering in a homogeneous/heterogeneous network: In a homogeneous network, the nodes in the same level are fully equivalent to each other. The sensor nodes are equivalent in initial energy, sensing limits, and communication limits. Therefore, in the same conditions, the sensor nodes have a similar response and every node can be a CH. In homogeneous networks, clustering algorithms are divided into two types: energy-based and hybrid parameters-based [14]. In a heterogeneous network, the sensor nodes differ in their efficiency, resources, energy, and power. Hence, the sensor nodes are classified into two classes: super-node and normal node. A super-node is a sensor node that has advanced hardware and high processing capability. The normal node has a lower capability. The CHs are selected from super-nodes. Heterogeneous networks are also divided into two types based on the parameters of CHs selection: energy-based and hybrid parameters-based [14].
- Energy-based clustering: To select the optimal cluster head in a heterogeneous network, in this type of algorithm, the sensor node with the highest energy level has the priority to be CH [14].
- Hybrid parameters-based clustering: the clustering algorithms select CHs based on different parameters, such as the size of the cluster, the neighbors' information, the distance between the nodes and the base station, etc. [14].

In the next paragraph, we will review some clustering algorithms and classify them according to the methodology and the parameters used in the clustering process.

3.2. Related Work

Many researchers have contributed to the development of clustering algorithms in WSNs and the utilization of all their advantages in various ways and all areas, such as security. In the following, many research papers interested in clustering algorithms are discussed. Zahedi et al. in [19] are interested in the low energy adaptive clustering hierarchy (LEACH) clustering protocol. It elects the CH among the nodes of the CH on the threshold equation randomly without regard to the energy of the nodes. Hence, the authors propose to enhance LEACH by modifying its threshold equation to consider the remaining energy to the maximum energy factor. The authors in [21] proposed a clustering algorithm where the selection of the CHs is based on the combination of a trust metric in addition to many other metrics. The trust metric relies on the behavioral aspect. It is based on direct and indirect observations of the node behavior. The factors used to assess the trust metric are the rate of the received acknowledged packets, the successful packets rate, the ratio of forwarding data, and the availability of nodes. Other metrics are used in the election process of CHs which are the waiting time of the node, its connectivity degree, and its relative mobility. Singh et al. [22] proposed a new clustering algorithm for WSNs with a practical swarm optimization (PSO) algorithm to enhance the lifetime of the network. The proposed algorithm consists of three phases: in the cluster formation with the PSO algorithm phase, the sink node is responsible for forming the clusters. Each node sends its identifier, location, and current energy level to the sink node. To ensure the effectiveness of the CHs selection, the sink computes the average energy level of each node. PSO is used by the sink node to identify the convenient number of CHs that minimizes the cost function. The inter-clusters communication phase establishes a path between the sensor nodes to transmit data. Finally, in the data transmission to the sink node phase, the CHs send data to the sink node.

The authors in [23] proposed an improved distributed energy-efficient clustering algorithm (IDEEC) for heterogeneous WSNs. The algorithm runs in rounds. First, the energy consumption is evaluated to define the minimum value for each round. Then, the IDEEC protocol evaluates the residual energy of the nodes and selects the CHs based on it. In the next step, IDEEC determines the optimal number of CHs in each round. To select the CH, a probability value is computed to ensure that the node having the highest energy level is selected CH and ensure that the total number of CHs is optimal. The authors in [24] proposed to detect, identify, and prevent the black hole attacks in mobile WSNs using a system built on a hierarchical cluster topology beside a trust model. The hierarchical cluster topology is composed of four levels including sensor node, CH, coordinator node (CO), and base station (BS). The network is divided into clusters, each cluster contains one or more CH and CO. The sensor nodes collect data and forward it to the CH. The CHs aggregate the data and forward it to the CO which, in turn, forwards it to the BS. The authors add a trust metric in the black hole attack detection mechanism, where the behavior of the nodes is assessed. The trust model is divided into two phases. First, the nodes discover their neighborhood and determine their trustworthiness by calculating the packet delivery ratio. Then, untrustworthy sensor nodes are revoked by adding them to a blacklist. The authors proposed in [25] a clustering algorithm named EPMS that uses the PSO algorithm. EPMS is used in the routing process to improve network performance. First, the network is divided into several regions using the PSO algorithm. Secondly, each sensor node calculates its distance from the center of gravity of the area. Thirdly, the average of remaining energy among all nodes of the region is calculated. Then, a node is elected CH if its remaining energy is greater than the average remaining energy for all nodes and it is the nearest one to the gravity center of the region. In [26], the authors proposed a black-hole detection model in WSNs-based applications in SG based on a clustering algorithm. The CHs are selected using trust factors. The trust factors are evaluated as a function of the energy, honesty, intimacy, and trade-off with dropped packets ratio. As consequence, only legitimate nodes are elected CHs. Minimizing energy consumption and enhancing network lifetime was the main goal of Fatima et al. [27]. They proposed an improved approach to

the weighted clustering algorithm by adding more specific parameters to the CHS election process, such as the distance between the nodes, remaining energy, and coactivity. The selection of the CHs is based on comparing the received signal strength indication (RSSI) and a predefined threshold. The sensor node that has an RSSI less than the predefined threshold is considered malicious, it is not eligible to be elected CH. Each non-malicious node computes a weight based on the aforementioned parameters, then broadcasts it in the network. The nodes with the highest weight become CH and other nodes are ordinary members of the cluster. In Table 1, we compare the clustering algorithms described above based on the following criteria:

- Cluster Size: the formed clusters may have an equal or unequal size that relies on the number of nodes in the cluster. In equal size clustering, all clusters have a fixed and predefined size, however, in unequal-size clustering, the clusters have variable sizes [27].
- Heterogeneity of the energy level: the heterogeneity level of WSNs is linked to the energy levels of the nodes. A two-level WSNs contains two energy levels for nodes named advance and normal node. The advance has more energy compared to a normal node [28].
- Heterogeneity: the WSNs are classified as homogeneous or heterogeneous based on the capabilities of the sensor nodes such as power, processing, and storage [29].
- CH selection: the CH can be selected using different parameters: Energy-based or hybrid-based. The selection may also be probabilistic or non-probabilistic.
- Routing approach: two approaches of routing are possible: classical routing and optimized routing. In classical routing, the selection of the base nodes is based on a timer function, which leads to irregular traffic flow in various base nodes. Optimized routing approaches are based on optimization algorithms, such as Fuzzy logic (FL), Genetic Algorithm (GA), and PSO [28].
- Clustering control: the control of the clustering in WSNs can be centralized or distributed. In the centralized approach, the sink node controls the clustering and needs global information (e.g., energy level) of the network. Moreover, it is responsible for the selection of the CHs. In a distributed approach, the sensor nodes cooperate to create the clusters [28].
- Inter-Clustering Routing: The sensor nodes and particularly the CH can communicate with the sink node in a single-hop or a multi-hop. In single-hop, the sensor nodes communicate directly with the sink node. However, in multi-hop, the sensor nodes communicate with the sink node via a mediator node in multi-hop routing [28].
- Intra-Clustering Routing: Member nodes can communicate with the CH in a single-hop or a multi-hop. In single-hop, the member nodes communicate directly with the CH, but in multi-hop, the member nodes communicate with it via a mediator node [28].

Table 1. Comparison of clustering algorithms.

Authors	Routing Approach (Classical, Optimized)	Control Manner (Centralized C, Distributed D)	Clustering Properties			Heterogeneity Homogeneous/ Heterogeneous Network	CH Selection				Energy Level Heterogeneity
			Clusters Size (Variable V/ Fixed F)	Inter-Cluster Routing	Intra-Cluster Routing		Probabilistic Hybrid Based	Probabilistic Energy-Based	Non- Probabilistic Hybrid Based	Non- Probabilistic Energy-Based	
Zahedi et al. [19]	Classical	D	V	Single-Hop	Single-Hop	Homogeneous	-	√	-	-	One Level
Singh et al. [22]	Optimized	C	V	Multi-Hop	Single-Hop	Homogeneous	√	-	-	-	One Level
B. Xie and C. Wang [23]	Classical	D	V	Single-Hop	Single-Hop	Heterogeneous	-	√	-	-	Multi-level
Pathak et al. [24]	Classical	D	V	Multi-Hop	Single-Hop	Heterogeneous	√	-	-	-	Multi-level
Wang, Jin et al. [25]	Optimized	C	V	Multi-Hop	Multi-Hop	Homogeneous	-	-	-	√	One Level
Otoum et al. [26]	Classical	C	V	Single-Hop	Single-Hop	Homogeneous	-	-	-	√	One Level
Belabed, Fatma, and Ridha Bouallegue [27]	Classical	C	F	Single-Hop	Single-Hop	Homogeneous	-	-	√	-	One Level
Rehman, Eid et al. [21]	Classical	D	V	Single-Hop	Single-Hop	Heterogeneous	-	-	√	-	Two-level
Proposed Algorithm	Classical	D	F	Single-Hop	Single-Hop	Homogeneous	-	-	√	-	One-level

3.3. Discussion

Table 1 shows many clustering algorithms based on different methodologies. We notice that the selection of CHs using an optimized-based approach is better in terms of fault tolerance, energy efficiency, and robustness as in [25]. To develop a secure clustering algorithm a trust metric must be considered, it may rely on many parameters, such as the packet delivery ratio [23], the received signal strength of the sensor nodes [27], and the successfully received packets rate [21]. In addition, considering the energy level is important to enhance the network lifetime. Table 1 shows that most of the studies consider the energy level in the selection of the CHs as in [19,23,25,26]. As shown in Table 1, in many clustering algorithms, inter and intra-clustering communications are single hop. Moreover, we remark that all the discussed protocols create variably sized clusters. Additionally, almost all clustering protocols are centralized approaches as in [22,25–27]. However, a variable size clustering leads to a non-balanced load on the CHs. In addition, the centralized approaches do not scale in the case of WSNs deployed in a SG because of the high number of sensors and the large deployment area. To overcome the aforementioned shortcoming of clustering in WSNs, we propose a new distributed clustering algorithm where the sensor nodes cooperate to create the clusters and elect the adequate CH based on a hybrid approach where different parameters are considered. The clustering process elects 1-hop clusters with a fixed size to balance the load on the CHs.

4. Methodology

4.1. Overview

To set up and maintain the credentials, the PKI is more efficient than the shared key, mainly for large-scale networks [9]. In a PKI, all devices have a unique pair of keys. Issuing, revoking, and updating the certificates is the responsibility of the CA. The PKI uses digital certificates to link the identities of the sensor nodes to a public key. The sensor node is being authenticated and recommended to the CA by the RA.

To cope with the problem of availability and scalability of centralized CA in SG environments, we propose to distribute the CA among many sensor nodes elected in the network using a clustering algorithm. Each cluster consists of one CA which is its CH, at least one RA, and many Members Nodes (MN) which are ordinary nodes belonging to the cluster. A CH must be a trustful node due to the sensitivity of its role in the cluster and to prohibit malicious nodes from competing in the CH election. In addition, a CH must have the highest energy level. Moreover, it must have at least two trustful neighbors. The RA must be also a trustful node, its role is to protect the CA from malicious nodes, and in case the CH is no longer CA in its cluster, the RA will replace it. The new clustering algorithm is detailed in the following section.

4.2. Clustering Algorithm

The clustering algorithm is based on different parameters to select the CHs. First, we consider the energy level of the sensor nodes to increase the clusters' lifetime. The second parameter is the degree of the sensor node defined as the number of its neighbors. A node having a degree less than two cannot be elected CH. In addition, a trust metric is considered in the election of the CH. The trust metric is a value in [0–1] that relies on the behavior of the node in terms of cooperation and authentic transmitted messages. A sensor node is considered trustful if its trust metric reaches 1. It must show a good attitude and good collaboration in the network to increase its trust metric. Many trust calculation techniques are proposed in the literature where the trust metric is evaluated based on the packet delivery ratio and RSSI [10,21,26].

The clustering algorithm goes through three main phases: discovery, clustering, and maintenance. In the discovery phase, all sensor nodes have to discover their neighborhood by exchanging HELLO messages with other sensor nodes. HELLO messages contain general information about the sensor node such as position, trust metric, and energy level. HELLO messages are periodically broadcast at 1-hop during a period TimerD.

Once TimerD expires, the sensor nodes move to the clustering phase. Each sensor node calculates the number of its neighbors called degree level DL. If the sensor is trustful, it has the highest energy level EL among its neighbors and at least two neighbors, it broadcasts an E-message to announce itself CH candidate, which means that it is eligible to be elected cluster head. Otherwise, the sensor node waits for an E-message from other CH candidates and tries to join one of them by sending a join request in a J-message. The collection of E-messages lasts for some time equal to TimerE.

Upon the expiration of TimerE, each candidate CH compares itself to other CHs candidates. If it has the highest energy level EL, the highest degree level DL and it has received at least one join request during TimerE, it announces itself CH in a HELLO message and accepts all the received join requests. Otherwise, the CH candidate joins another CH. It is worth mentioning here that all the clusters have a fixed size measured by the maximum number of member nodes. Figure 1 shows the flowchart of the proposed algorithm.

Later on, if a new sensor node joins the network, it may receive HELLO messages from existing CHs. In this case, it sends a join request to the nearest one. If the sensor node does not receive an acknowledgment during a TimerA, it sends a J-message to another CH. Once a sensor node becomes a member of a cluster, its role depends on its trust metric. If it is trustful and located at 1 hop from the CH, it will be a RA, otherwise, it is an ordinary member node.

In the maintenance phase, each CH sends periodic HELLO messages to the members of its clusters to make them aware that is always alive. At the same time, the RA nodes send periodic HELLO messages to their CA. The CA is still alive if it has at least one RA in the cluster, otherwise, it will be no longer CA and a re-clustering process should take place.

4.3. The Characteristics of the Proposed PKI

The clustering algorithm allows us to build a distributed and self-organized PKI. Each cluster consists of one CA, one or more RA, and a lot of ordinary MNs. Their roles are described as follows:

- CA: it is the CH of the cluster. Its role is to manage short-term certificates for RAs and MNs.
- RA: it is a truthful node at 1 hop of the CA. Its role is to check certification requests received from MNs before forwarding them to the CA. The certification request is valid only if the requester node has a valid long-term certificate.
- MN: It is a regular node with no particular role in the cluster.

We suppose that initially, all the sensor nodes have long-term certificates issued offline by a centralized CA, it is useful to authenticate the sensor nodes upon their entry into the network. Generally speaking, in a traditional PKI, all sensor nodes need to periodically communicate with the centralized CA to renew their certificates and avoid spoofing attacks. Since the considered WSN is deployed in a SG environment characterized by its wide area of coverage, a large number of sensor nodes, and the intermittent connection, this frequent communications risk failing, consequently, the sensor node will not be able to cooperate with its neighbors. To mitigate this problem, in the proposed architecture each sensor node belonging to a cluster asks for a short-term certificate from its CH, this certificate will be used to communicate within the cluster. If the sensor node is compromised or it needs to renew its expired short-term certificate, it must contact its CH. The CH issues the short-term certificate to the sensor nodes in its cluster after authenticating them using their long-term certificate. On one hand, this will reduce the delay in renewing the long-term certificates. On the other hand, it will avoid spoofing attacks. If the key of the sensor node is compromised, it can be easily and quickly revoked by the CH and a new certificate is issued instead of contacting the centralized CA.

The new distributed architecture of the PKI circumvents many issues of the centralized approach. First, it allows the avoiding of the problem of a single point of failure by distributing the role of the CA among many sensor nodes elected based on many parameters that rely on the network topology. If one CA is compromised or no longer available, the

certification process fails only in one cluster. More importantly, the RA sensor node will play a crucial role in the availability of the CA. Particularly, their role consists of filtering the certification requests intended for the CA and avoiding DoS attacks on it. The clustering process is based on a trust metric that allows filtering out malicious nodes upon the election of the CA. In addition, the asymmetric encryption feature provides non-repudiation, authentication, and confidentiality. Furthermore, the use of short-term certificates allows the mitigation of the sinkhole and Sybil attacks. Instead of storing short-term keys in the CA, periodically the sensor node renews its keys by contacting the CA in its cluster.

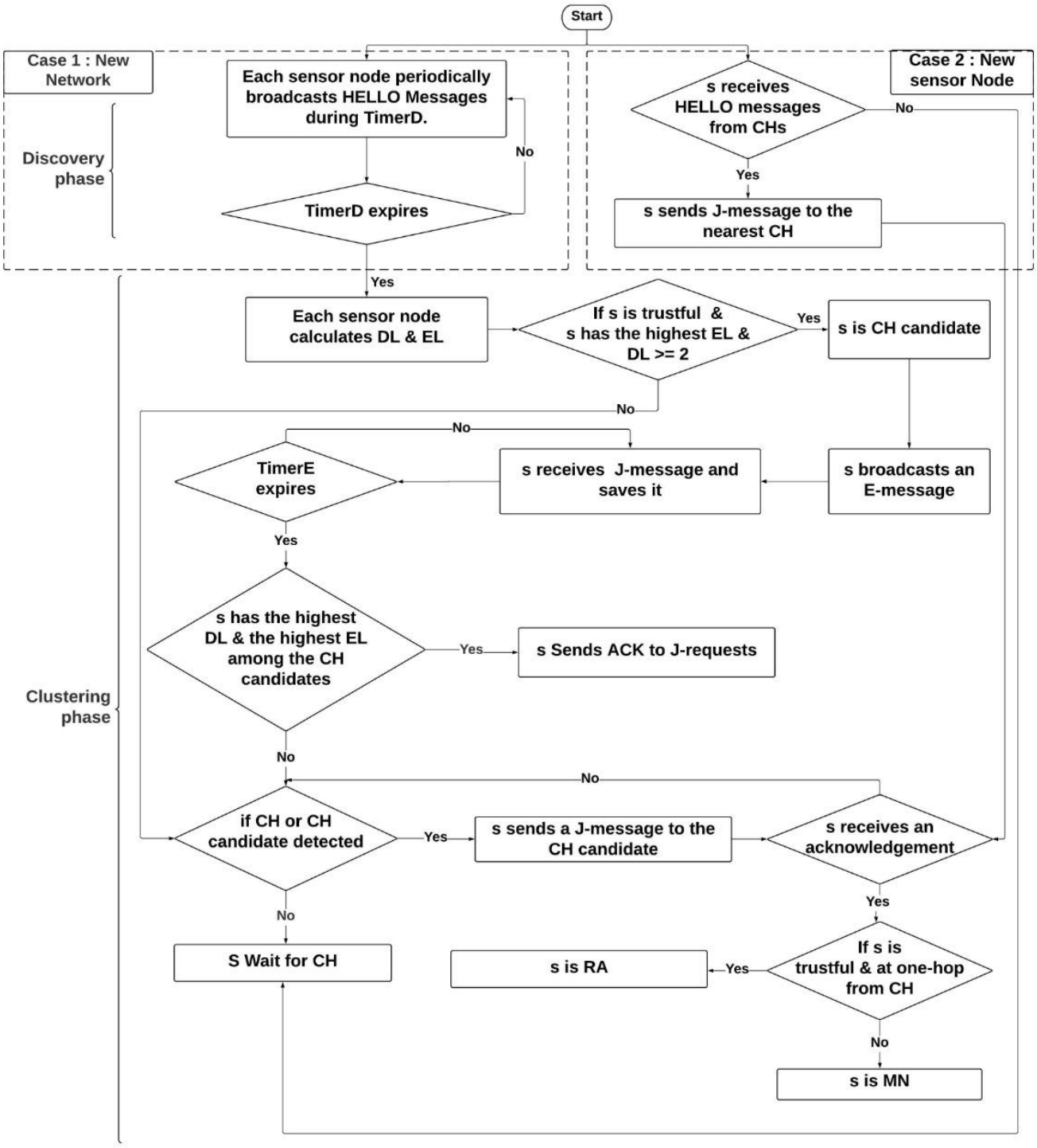

Figure 1. Flowchart of the proposed clustering algorithm.

5. Results

In this section, we will investigate the performance of the proposed clustering algorithm in terms of scalability and efficiency.

5.1. Simulation Setup

We have used the network simulator OMNET++. It is composed of modules written in C++ that connect through message passing [30]. The clustering algorithm has been implemented in the WSNs library Castalia [31]. Castalia provides developers and researchers with a trustworthy framework to validate their distributed algorithms before implementing them in real WSNs.

To investigate the performance of the proposed clustering algorithm, we have considered a network with an average of 200 nodes deployed as a grid in a network size of 100 × 100 m. Table 2 shows the simulation parameters.

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

5.2. Simulation Results

First of all, we will investigate the number of elected CA. To this end, we plot, in Figure 2, the number of CA as a function of the number of nodes in the network. We observe that whenever the number of sensor nodes in the network increases, the number of elected CA increases also. It passes from 5 for 150 nodes in the network and a cluster size of 30 nodes to 6 clusters for 200 nodes. All the clusters have a fixed size which relies on the maximum number of members, if a cluster is saturated, a new cluster will be created. It is obvious also from Figure 2 that the size of the cluster affects the number of CAs, if it increases the number of CA decreases. This points out that the proposed clustering algorithm always selects the minimum number of CAs necessary to allow all nodes to join the clusters as we will show later. A new cluster is created only if the existing clusters are full.

Figure 3 shows the impact of the transmission range on the number of elected CA. Since the proposed algorithm is designed to fit into a SG environment where the number of sensors in the network is high at the same time the sensors will be widespread in the plant, we have opted to use high transmission range values (more than 50 m).

As shown in Figure 3 the number of CA is notably decreasing when the transmission range increases. Indeed, 18 clusters are created for a transmission range of 50 m however only 10 clusters are created in the case of 250 m for a total of 250 sensor nodes in the network and a cluster size of 25. This result can be explained by the fact that when the transmission range of the sensor nodes increases, far sensor nodes will be able to detect the CA. Hence, fewer CHs will be elected, and consequently fewer clusters will be formed. It is worth mentioning that the more the transmission range increases, the more energy will be consumed, that is why we have opted for a maximum of 250 m in Figure 3.

Figure 4 shows the number of CAs as a function of the percentage of malicious sensor nodes in the network. It is obvious in Figure 4 that the percentage of malicious nodes in the network does not affect the number of CA. The number of CA is constant on increasing the number of malicious nodes for two reasons: the election of the CA is based on a trust metric that reflects the trustworthiness of the node, so a malicious node will not be able to become a

CA. The second reason is that the join requests coming from the sensor nodes to the CA are filtered by the registration authority to avoid any compromise of the certification authority.

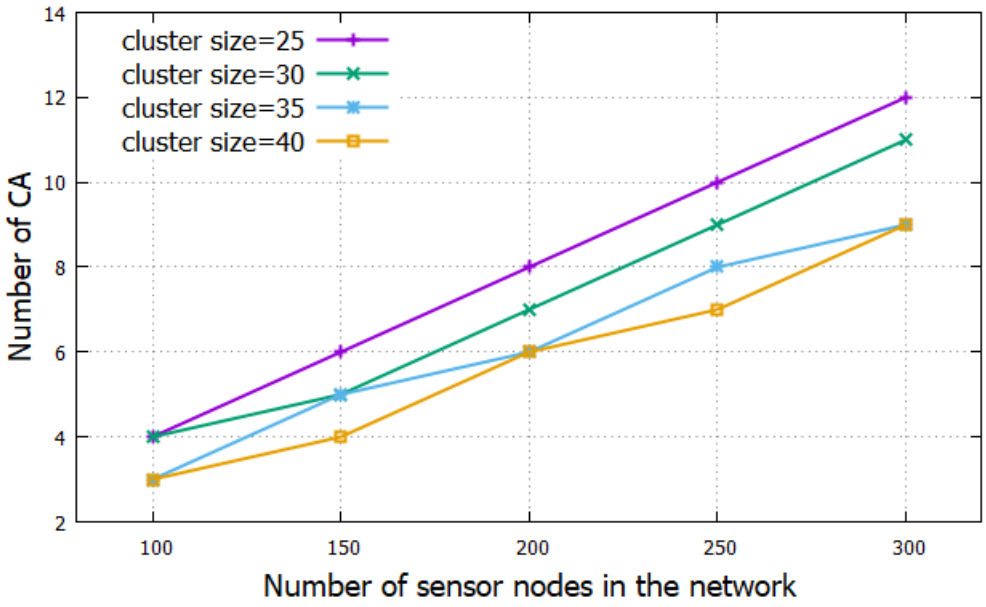

Figure 2. The number of CA as a function of the number of sensor nodes in the network.

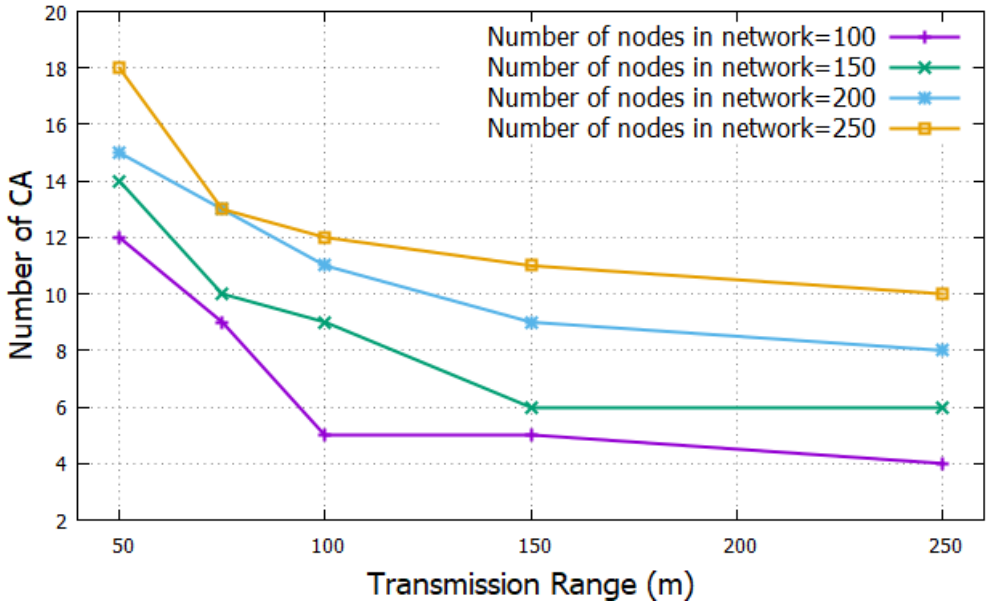

Figure 3. Number of CA as a function of the transmission range.

Figure 5 presents the percentage of malicious sensor nodes elected CAs as a function of the number of malicious nodes in the network for the proposed algorithm as well as a clustering algorithm entitled Energy Efficient Secure trust-based (EEST) [20] described in the related work section. Figure 5 shows that around 10% of malicious sensor nodes are elected CAs in EEST while none of the malicious sensor nodes is elected CAs in the proposed algorithm. This feature is due to the trust metric used in the election process. Only trustful sensor nodes can be elected CAs in the proposed algorithm.

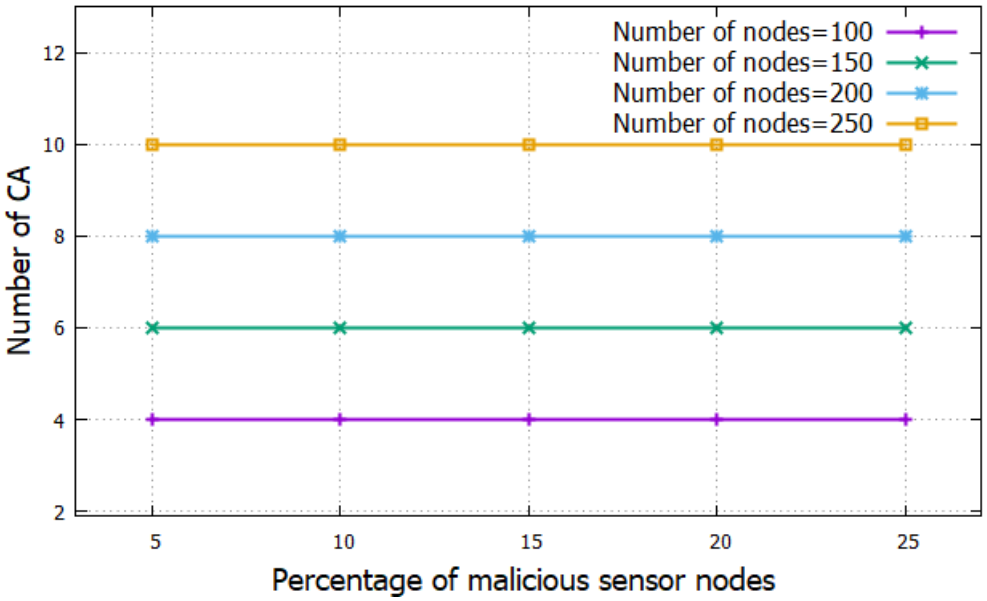

Figure 4. Number of CA as a function of the percentage of malicious sensor nodes in the network.

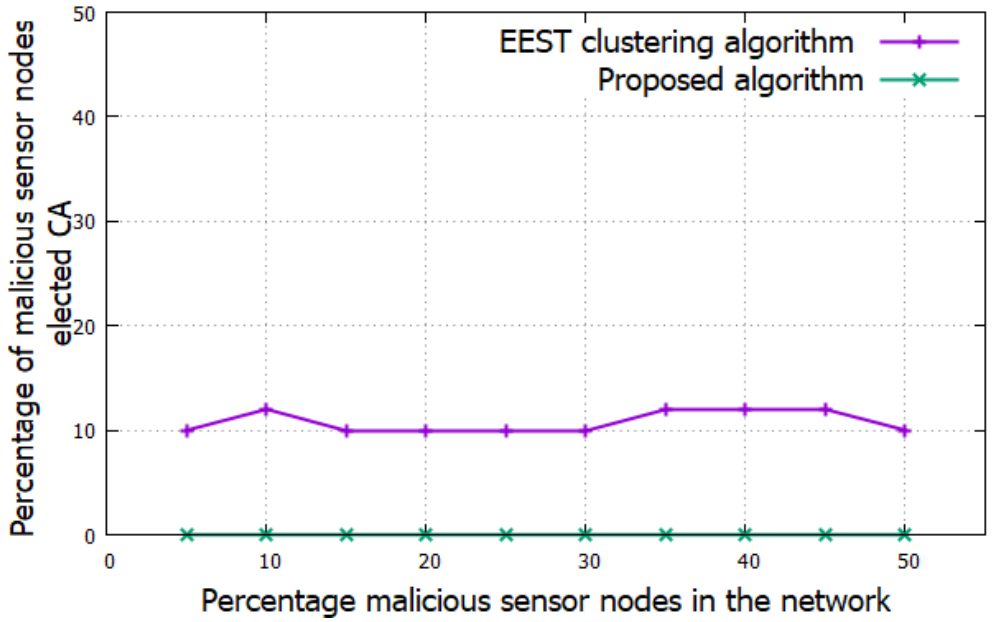

Figure 5. The percentage of malicious sensor nodes elected CA as a function of the total number of malicious sensor nodes in the network.

Figure 6 shows the percentage of sensor nodes that are members of the clusters as a function of the total number of sensor nodes in the network. We notice that when the transmission range is equal to 100 m around 2% of the nodes are not in clusters. On one hand, this may be due to their short transmission range or they are deployed in the network extremities, which makes them unable to join the existing CA. On the other hand, if they are malicious, they cannot create a cluster. In addition, it is obvious from Figure 6 that the percentage of member nodes in the clusters is 100% for higher transmission ranges. This result confirms the efficiency of the proposed clustering algorithm and shows that the number of clusters created covers the network area.

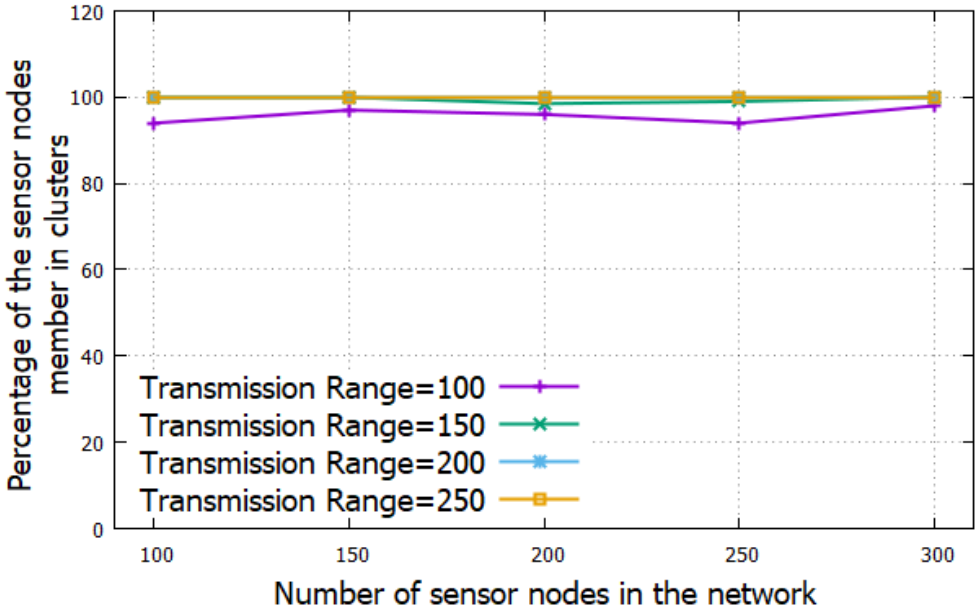

Figure 6. Percentage of the sensor nodes member in clusters as a function of the number of nodes in the network.

We plot, in Figure 7, the energy consumption level as a function of the number of nodes in the network. On one hand, we notice that the energy consumption of CA is slightly higher than the energy consumption of other sensor nodes. This result points out that the role of CH does not need extra energy consumption. Although, it will send periodic HELLO messages and join acknowledgments. On the other hand, we remark that the higher the number of sensor nodes in the network, the higher the energy consumption level is because the sensor nodes will exchange more HELLO messages and control messages to form the clusters. Though, the energy consumption does not exceed 1% of the initial energy of the sensor.

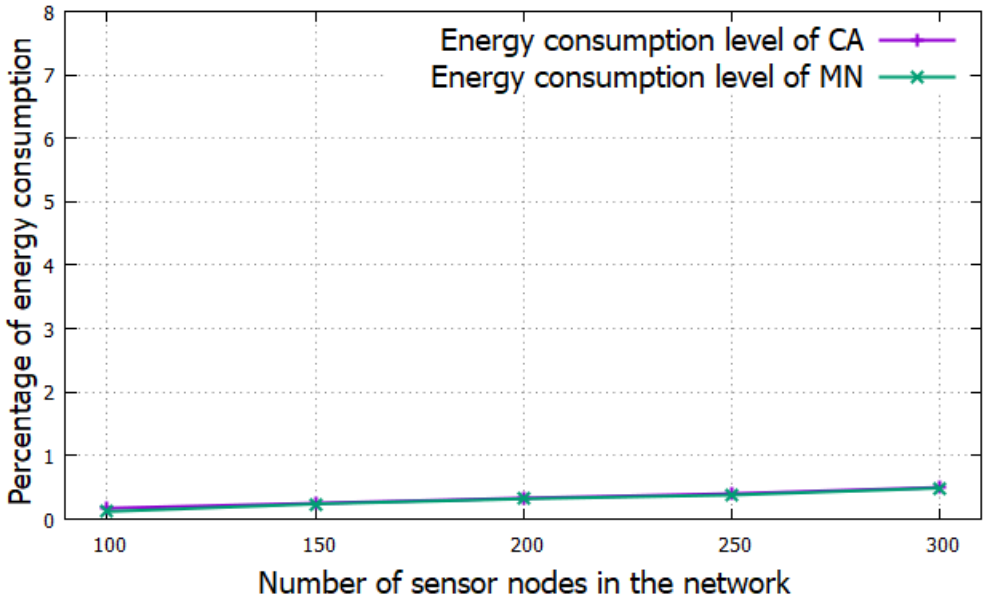

Figure 7. The percentage of energy consumption as a function of the number of sensor nodes in the network.

Figure 8 shows the lifetime of the cluster head as a function of the percentage of malicious sensor nodes. The lifetime of the CA relies on having at least one RA in the

cluster and having a sufficient energy level. Figure 8 shows that the lifetime of the CA is 100%, which means that it will be alive during all its journey in the network. This result confirms the stability of the proposed clustering algorithm in terms of cluster lifetime, a sensor node will rarely need to change its cluster.

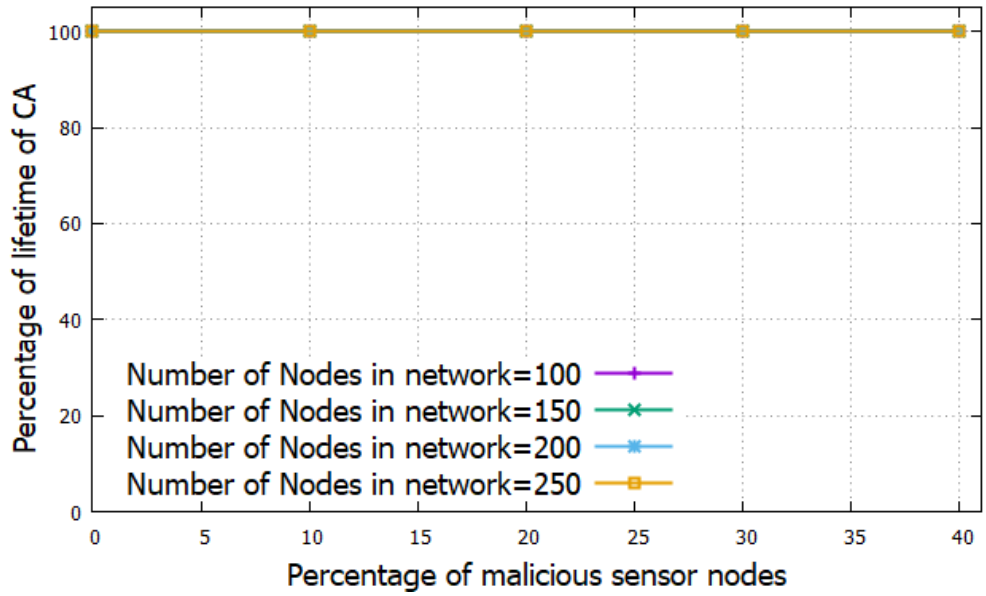

Figure 8. The lifetime of the CA as a function of the percentage of malicious sensor nodes.

6. Conclusions

In this paper, we propose a new security architecture for WSN-based applications in SG. The architecture consists on a distributed PKI where the role of the centralized CA is delegated to a set of sensor nodes dynamically elected in the network using a clustering algorithm. The objective is to ensure that the CA services are available as long as possible and to overcome the problem of a single point of failure of the centralized CA. The clustering algorithm is based on a trust metric that reflects the behavior of the sensor nodes; if one CA is compromised, only its cluster will be affected. The simulation results show that almost all sensor nodes are members of clusters. Furthermore, the lifetime of the elected CA is high which confirms the stability of the distributed PKI. In addition, the proposed architecture is scalable, the more sensor nodes enter the network, the more clusters are created which avoids any denial of service on the existing CAs. From a security perspective, the proposed architecture allows the establishment of secure communications among the sensor nodes. Having a legitimate certificate and keys will allow mitigating against Sybil attacks in addition to the encryption which avoids eavesdropping.

In our future work, we expect to design a trust management framework for WSN in SG aiming to assess and maintain the trust metrics of the sensor nodes. Furthermore, the inner processing of the PKI will be developed particularly the certification and revocation processes.

Author Contributions: Methodology, T.G.; Validation, T.G.; Resources, N.A.; Writing—Original Draft Preparation, N.A.; Writing—Review and Editing, T.G. All authors have read and agreed to the published version of the manuscript.

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

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. 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*, 4025–4047. [CrossRef]
2. 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, Mykonos, Greece, 27–30 September 2015.
3. Mehmood, G.; Khan, M.S.; Waheed, A.; Zareei, M.; Fayaz, M.; Sadad, T.; Kama, N.; Azmi, A. An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network. *Complexity* **2021**, *2021*, 6577492. [CrossRef]
4. Amutha, J.; Sharma, S.; Sharma, S.K. 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. [CrossRef]
5. 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*, 5. [CrossRef]
6. Liu, Y. Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenges. *Int. J. Distrib. Sens. Netw.* **2012**, *8*, 1–8. [CrossRef]
7. 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, Adelaide, Australia, 6–9 December 2011; pp. 359–364. [CrossRef]
8. Nandhini, M.; Praveenkumar, B. An Implementation of Public Key Infrastructure Using Wireless Communication Networks. *Int. J. Grid Distrib. Comput.* **2015**, *8*, 35–42.
9. Mahmoud, M.M.E.A.; Mišić, J.; Shen, X. A scalable public key infrastructure for smart grid communications. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 784–789. [CrossRef]
10. 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*, 10–16. [CrossRef]
11. Shahzad, F.; Pasha, M.; Ahmad, A. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. *IJCSIS* **2017**, *14*, 54–65.
12. Kivande, M.V.; Wade, A.M. Adaptive and Channel Aware Forwarding Attack Detection for Mobile Sensor in WSN with Security of Data. *Int. J. Eng. Sci.* **2017**, *7*, 13256.
13. Riaz, M.N. Clustering algorithms of wireless sensor networks: A survey. *Int. J. Wirel. Microw. Technol.* **2018**, *8*, 40–53.
14. Rostami, A.S.; Badkoobe, M.; Mohanna, F.; Keshavarz, H.; Hosseinabadi, A.A.R.; Sangaiah, A.K. Survey on clustering in heterogeneous and homogeneous wireless sensor networks. *J. Supercomput.* **2018**, *74*, 277–323. [CrossRef]
15. Fanian, F.; Rafsanjani, M.K. Cluster-based routing protocols in wireless sensor networks: A survey based on methodology. *J. Netw. Comput. Appl.* **2019**, *142*, 111–142. [CrossRef]
16. Arjunan, S.; Sujatha, P. A survey on unequal clustering protocols in Wireless Sensor Networks. *J. King Saud Univ.-Comput. Inf. Sci.* **2019**, *31*, 304–317. [CrossRef]
17. Zeb, A.; Islam, A.K.M.M.; Zareei, M.; Al Mamoon, I.; Mansoor, N.; Baharun, S.; Katayama, Y.; Komaki, S. Clustering Analysis in Wireless Sensor Networks: The Ambit of Performance Metrics and Schemes Taxonomy. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 1–12. [CrossRef]
18. El Khediri, S. Wireless sensor networks: A survey, categorization, main issues, and future orientations for clustering protocols. *Computing* **2022**, *104*, 1–63. [CrossRef]
19. Zahedi, A. An efficient clustering method using weighting coefficients in homogeneous wireless sensor networks. *Alex. Eng. J.* **2018**, *57*, 695–710. [CrossRef]
20. Koucheryavy, A.; Salim, A. Cluster head selection for homogeneous Wireless Sensor Networks. In Proceedings of the 2009 11th International Conference on Advanced Communication Technology, Gangwon, Korea, 15–18 February 2009.
21. Rehman, E.; Sher, M.; Naqvi, S.H.A.; Khan, K.B.; Ullah, K. Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network. *J. Comput. Netw. Commun.* **2017**, *2017*, 1630673. [CrossRef]
22. Singh, S.P.; Sharma, S.C. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI—2018), Madurai, India, 19–20 December 2018*; Springer International Publishing: Cham, Switzerland, 2020; pp. 1775–1780.
23. 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), San Francisco, CA, USA, 19–22 March 2017.
24. Pathak, G.R.; Patil, S.H.; Tryambake, J.S. Efficient and trust based black hole attack detection and prevention in WSN. *Int. J. Comput. Sci. Bus. Inform.* **2014**, *14*, 93–103.
25. Wang, J.; Cao, Y.; Li, B.; Kim, H.-J.; Lee, S. Particle swarm optimization based clustering algorithm with mobile sink for WSNs. *Futur. Gener. Comput. Syst.* **2017**, *76*, 452–457. [CrossRef]
26. Otoum, S.; Kantarci, B.; Mouftah, H.T. Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017. [CrossRef]
27. 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), Paphos, Cyprus, 5–9 September 2016; pp. 757–762. [CrossRef]

28. 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. [CrossRef]
29. Velmurugan, S.; Logashanmugham, E. Secure Mobile Beacon Based Obstacle Awareness in WSN. *Inst. Integr. Omics Appl. Biotechnol.* **2017**, *8*, 1–7.
30. Varga, A. Using the OMNeT++ discrete event simulation system in education. *IEEE Trans. Educ.* **1999**, *42*, 11. [CrossRef]
31. Castalia. Available online: http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/INGRES-M1/Castalia%20-%20User%20Manual.pdf (accessed on 25 October 2021).