المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثالث والأربعون (شهر 12) 2021

Defense Mechanism Against Sybil Attack in Wireless Sensor Networks

Athari Mohammed Alrajhi
Computer Science Lecturer, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
amalrajhi@iau.edu.sa

ABSTRACT

Security has become a most critical issue for several wireless sensor networks applications. The ad-hoc nature of wireless networks and the deployment of sensor nodes in hostile areas make them vulnerable to several types of attacks. One of the most severe attacks in wireless networks is the Sybil attack in which a malicious node illegitimately claims multiple identities.

Sybil attack can destroy the routing mechanisms such as LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol which is used to provide the function of data routing towards the base station by partitioning the sensor nodes into clusters. Also, Sybil attack poses a threat to cluster-based networks, because once the Sybil node becomes a cluster-head, it has a harmful effect on not only neighbor nodes

but also the whole cluster. This adverse effect degrades data integrity, security, and resource utilization.

In attempting to protect wireless sensor networks against such an attack as well as to enhance the network security, we propose a novel detection scheme of Sybil attack in a clustering-based hierarchical network. Our proposed approach can detect the Sybil node which behaves as a cluster-head in wireless networks. The method is based on the RSSI (Received Signal Strength Indicator) technique to determine the location of the nodes without any additional specialized hardware/software.

Keywords: Sybil Attack, Wireless Sensor Network, Defensive mechanisms, LEACH protocol, Security, RSSI.

1. Introduction

A wireless sensor network (WSN) is a network that consists of base stations and a large number of nodes where each node is equipped with a sensor to monitor physical or environmental conditions like light, heat, pressure, etc. WSNs provide an ideal solution for a variety of monitoring and surveillance applications such as pollution sensing, wildlife monitoring, military target tracking and traffic monitoring. The majority of these applications requires security, especially for critical infrastructures. Limited energy, storage and computational resources of sensor nodes [1] make the implementation of security techniques in WSNs complicated. Therefore, sensor networks have become vulnerable to various attacks.

Sybil attack is one of the severe attacks, which poses a serious threat to the integrity of WSNs. It is an active routing attack which monitors, listens to and modifies the data stream in the communication channel, and acts on the network

layer while routing the messages. It was originally described as an attack able to defeat the redundancy mechanisms of distributed storage systems in peer-to-peer networks [2]. In such an attack, a single node (malicious node) presents multiple identities to other nodes in the network. This is done by either claiming false identities or simply stealing legal identities of other sensor nodes [1]. It is common to refer to a malicious device's additional identities as Sybil nodes. The Sybil node tries to communicate with neighboring nodes by using the identity of the legitimate node. This confuses and collapses the network. Figure 1.1 shows a scenario of Sybil attack in WSNs. The Sybil nodes typically have the same set of neighbors because they are all associated with the same physical device (i.e., the malicious node). This characteristic of Sybil nodes was exploited to detect a Sybil attack by collecting neighboring information and then analyzing the results.

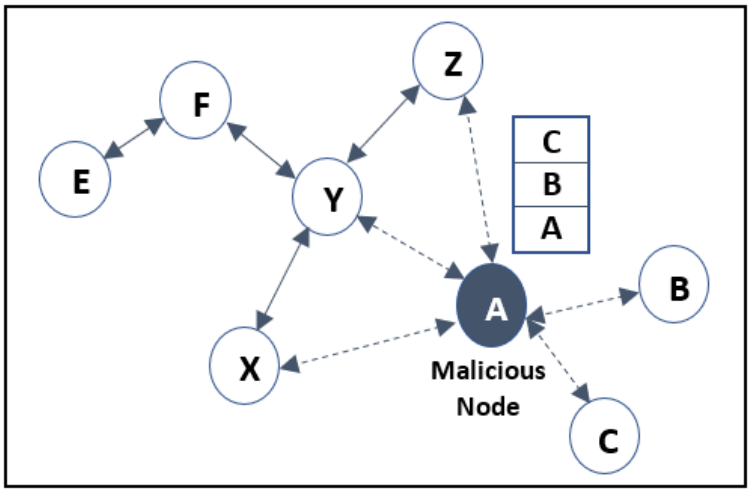

Figure 1.1: Sybil Attack

Also, Sybil attack can be used against clustering-based routing protocols [3] like LEACH protocol. Such protocols organize the sensor nodes in groups called clusters to report data from the cluster members to the cluster head and in turn, transfer it to a centralized base station. Sybil nodes may attack routing mechanisms in order to transmit the packets to an incorrect destination. These threats by Sybil attack have made the need for security very important to protect the network from such attack.

1.1. Problem Statement

We assume a static wireless sensor network, where all sensor nodes are immobile after initial deployment. Given a set of cluster heads, member nodes and a base station which are deployed in a geographical region such that a Sybil node can capture and tamper a benign cluster-head for the purpose of converting it as malicious that can launch Sybil attack. Once the Sybil node becomes a cluster-head, it has a bad effect on not only neighbor nodes but also the whole cluster. This harmful effect degrades data integrity, security, and resource utilization. In response to this problem, our study proposes to investigate a new defense mechanism to detect the malicious cluster-head, which has the intention of causing the Sybil attack in the wireless sensor network.

1.2. Motivation

Advances in the wireless communications field led to an increasing interest in wireless sensor networks in recent years. WSNs provide an ideal solution for a variety of monitoring applications. These applications require security to protect the network from attacks such as Sybil attacks. Therefore, Sybil attacks have been widely studied by the researchers and proposed several defense schemes. However, existing techniques require costly requirements such as nodes position [4], encryption keys [5] and identity certificates [6] methods. However, these techniques increase overhead and not suitable for the limited resources of the sensor nodes. Therefore, an efficient scheme is required to detect Sybil attacks without additional overhead as well as to conserve energy and prolong the network lifetime.

1.3. Contribution

This paper is focused on a promising mechanism to mitigate Sybil attack in WSNs using RSSI technique. Our solution can detect the malicious cluster-head that may cause the Sybil attack. The proposed approach does not require any

special requirements or shared keys to detect the Sybil node. Furthermore, we analyze and compare the existing defense mechanisms against Sybil attack.

1.4. Paper Organization

The remainder of the paper is structured as follows. The background section presents the basic information of clustering concept, LEACH protocol and RSSI technique. The literature review section discusses the related work on Sybil attack from a security perspective and possible countermeasures. The proposed scheme, network model and assumptions are described in proposed approach section. Finally, conclusion section concludes the work and presents some directions for future work.

2. Background

The network structure is categorized into flat and hierarchical approaches. In flat networks, all sensor nodes cooperate with each other in order to route the data to the base station, which each node has the same role. In hierarchical approaches, sensor nodes are clustered into groups to save the energy of nodes during the routing process. This function can be performed by several routing protocols such as LEACH protocol.

In this section, we provide the most important information concerning the concept of clustering in wireless sensor networks as well as the function of LEACH protocol and its importance in routing data in hierarchical networks. In addition, we present the RSSI technique as a function of distance in WSNs.

2.1. Clustering in WSNs

Clustering is an important technique in large wireless sensor networks for reducing energy consumption, increasing network lifetime and achieving better network performance [7]. It is an energy efficient routing mechanism that transfers data from the sensor nodes to a centralized base station. All the sensor

nodes in a network organize themselves into groups called clusters. One of these nodes in each cluster acting as the cluster-head (CH). The rest of the nodes (non-cluster-head nodes) transmit their data to the cluster-head. The latter receives and aggregates data from its member nodes (MN) (intra-cluster communication), and cooperates with other cluster-heads to transmit data to the base station (inter-cluster communication). Figure 2.1 shows clustering network topology.

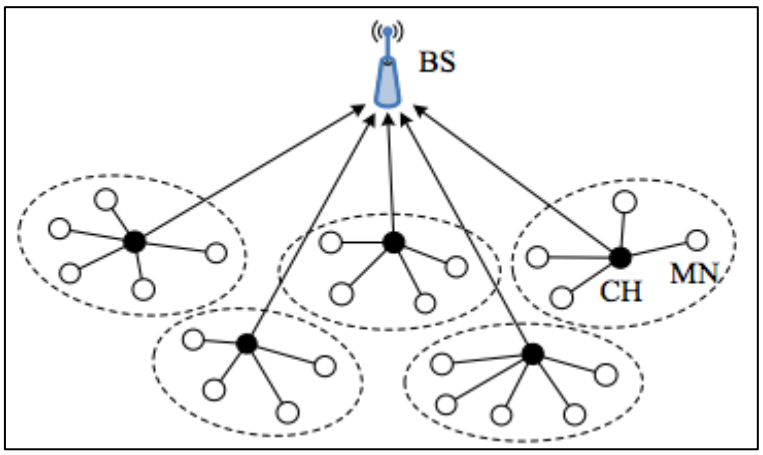

Figure 2.1: Clustering in WSNs [7]

2.2. LEACH Protocol

Due to energy consumption during routing process in flat networks, dynamic LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol [8] is used to provide the function of data routing towards the base station with low energy consumption by partitioning the sensor nodes into clusters. This function is implemented in two phases. The first one is the Setup phase where cluster-heads are chosen randomly and the formation of clusters with cluster-heads and member nodes is done for the WSNs. Each node in the network becomes a cluster-head at least once. While in Steady phase, data is collected and transmitted to the base station.

2.3. RSSI

RSSI stands for Received Signal Strength Indicator. It is a measurement of the power present in a received radio signal, and can be measured in any unit of

power. It is often expressed in decibels (dB), or as percentage values between 1-110, and can be either a negative, or a positive value. This technique is used in WSNs to estimate the distance between nodes wirelessly [9].

3. Literature Review

Sybil attacks can destroy the network integrity and compromise the security by disabling many networking protocols such as routing protocols. So, security against Sybil attack has been able to attract the attention of many researchers around the world. They proposed several approaches in order to avoid the threat of Sybil attack, or at least limit its consequences. According to [10], [11], [12] and [13], these proposed approaches are classified into five categories including resource testing, trusted certification, position/ location verification, RSSI-based scheme and random key pre-distribution. This classification is based on the method or technique which is used to detect the Sybil attack.

In this section, we review various mechanisms proposed to prevent and mitigate the Sybil attack in wireless sensor networks. In addition, we present a brief discussion and comparison of the existing methods. The approaches have been summarized and presented according to the previous classification as follows.

3.1. Approaches

3.1.1. Resource Testing

Resource Testing is the most common solution to avoid Sybil attacks. The threat of Sybil attack was first studied by Douceur in the context of peer-to-peer networks [2]. In the absence of an identification authority, peer-to-peer systems will be susceptible to Sybil attacks, in which some entities forge multiple identities to compromise the system. Douceur proposed a resource testing method which assumes that a local entity's ability to discriminate among distinct remote entities depends on that an attacker's resources are limited. The method tests

whether each identity has as many resources as the single physical device it is associated with. Any discrepancy indicates the possibility of a Sybil node. These tests include storage, computing, and communication resources. Computation and storage are inappropriate for WSNs because the attacker might have these resources in large capacities compared to resource-starved sensor nodes. The proposed method of testing communication is to send a message to identities and then only accept replies that occur within a certain period. This method is also unsuitable for WSNs because the messages used for verifying communication resources might flood the entire system itself. Newsome et al. [1] studied the same problem in the context of wireless sensor networks. Their proposed method is based on the radio resources used by a node. It assumes that any device has only one radio and this radio is incapable of sending or receiving on more than one channel at a time. If a node wants to verify that none of its neighbors are Sybil nodes, it assigns each of its neighbors a different channel to send a message on. Then, it will choose a channel to listen. If the neighbor node that was assigned that channel is a legal node, it should hear the message. The results showed the effectiveness of the method in the simulation environment. Whereas, attackers in the real-world environment may have multiple channels. But in general, these results are better than the results obtained by Douceur [2].

In the clustered sensor network topology, Sinha et al. [13] used the previous idea of node resources with some modifications to be suitable for clustering networks. Their method starts with suspecting a node as Sybil if it has a maximum number of packets drop and then verifies it by two phases. In the first phase, the observer (single node) makes a cluster and calculates the dissimilarities between the nodes. Then, the observer constructs a graph in which the node with maximum connected components is taken as Sybil node. In the second phase, the similarities between the nodes are calculated. Then, the graphs are plotted in the same manner as in the first phase. If the result of both phases indicates that the same node is Sybil node,

then the node is really a Sybil one. This method has demonstrated its ability to combine clustering and using of node resources effectively in order to detect Sybil attack.

3.1.2. Trusted Certification

Trusted certification is by far the most frequently cited solution to defeating Sybil attacks. Douceur [2] has proved that such kind of certification is the only method that has the potential to eliminate Sybil attacks completely. This approach relies on a centralized authority CA that verifies the validity of each node, and issues a certificate for the honest one. Centralized authority thus eliminates the problem of establishing a trust relationship between two communicating nodes. In fact, Douceur does not offer any method for ensuring such uniqueness, and in practice, this technique is costly because it needs a manual configuration to perform it in large-scale systems. To get better results in large systems, Saha, H et al. [14] proposed another technique based on using RSSI value with trusted certification to detect Sybil nodes. They assume that the network will be divided into several subgroups. Each subgroup will contain a central authority (a single trusted node) and RSSI detector nodes. If the detector nodes declare Sybil attack, the trusted node checks whether the node is indeed a Sybil node or not. If so, it is removed. When the number of nodes exceeds a threshold value, a new subgroup will be created, and a new trusted node will be assigned as the central authority of that subgroup. The technique proved its ability to detect Sybil nodes in large networks. But the problem associated with it, that the central authority can easily become a target for Sybil attack.

The idea of threshold value with trusted certification is also used by R. Singh et al. [6]. They proposed a novel approach called a Trust-Based Sybil Detection (TBSD) to detect Sybil nodes in WSNs. The scheme is based on trust values of adjacent sensor nodes. The nodes with the trust values less than a threshold value

are detected as Sybil node. The experimental results show that the TBSD attains significant attack detection rate than previous techniques.

In cluster network topology, SRSRP (Sybil Resistant Secure Routing Protocol) has been proposed by H. Singh, et al. [15] to protect the cluster head against Sybil attack. In this approach, the base station (BS) is considered a central authority which is used to verify the identity of the cluster head. Any node wants to be a cluster head, it will send its ID and an encrypted message using Armstrong number to BS and in turn, decrypts the message using the same Armstrong number. If the message is not decrypted or ID is not found in the registration table, it means that the node is a Sybil node. The simulation results showed the efficiency of the proposed protocol for the detection of Sybil attack. However, the malicious node may penetrate the authentication mechanism.

3.1.3. Position/ Location Verification

This technique is based on the fact that the same position in a network should not be occupied by more than one identity simultaneously. It checks the location of each identity by using distance measurement.

Mukhopadhyay and Saha [4] proposed a location verification based defense against Sybil attack. This method assumes the presence of an agent who is aware of the locations of all nodes. When a new node joins the network and claims its position, then agent verifies the claimed location. If the claimed location fabricated, the node is considered a potential Sybil node. Although this method needs special requirements such as software agent and the awareness of nodes locations, the results showed their ability to defend against Sybil attack. In another study, Vamsi and Krishna [16] suggested a lightweight Sybil attack detection framework (LSDF). The proposed framework is based on evidence theory which includes evidence collection and validation. It works with information of neighboring nodes observed by each node to collect evidences. Observations,

distance and RSSI values of nodes are recorded during the evidence collection. These evidences are submitted and verified by running sequential ratio test to decide easily whether neighboring node is a Sybil node or legitimate node. With extensive simulations, it was showed that the LSDF could detect Sybil attack with few evidences. Meanwhile, it consumes too much energy than [4].

The Sybil nodes typically have the same set of neighbors because they are all associated with the same physical device (i.e., the malicious node). This characteristic of Sybil nodes was exploited to detect a Sybil attack by collecting neighboring information and then analyzing the results. This technique has been adopted by Ssu et al. [17]. They proposed a detection scheme which executed by a normal node N. N sends a message to one of its neighbors I, and the latter broadcasts a message over its maximum transmission range. Any node is hearing this message, replies using one hop broadcast directly to N. Then, N records the IDs of the nodes which send a reply and combines these IDs to form the set of common neighbors for both N and I. The process is repeated until all of the set has been collected. N will then compute the total number of appearances of each node. Therefore, if the number of appearances of a node exceeds a certain threshold value, the node is considered a Sybil node since the amount of Sybil nodes is large. The simulation results have shown that the Sybil nodes can be correctly identified, with a false detection rate of 4%. However, the computations may consume the energy of the nodes, which is the same problem in [16].

To avoid the energy consumption problem in previous methods, an energy efficient integrated intrusion detection system is proposed by Karuppiah et al. [18] to detect network layer Sybil attack. This scheme spends less energy when detecting the Sybil node which behaves as a normal node in clusters. The CH creates a table of all nodes with their IDs and positions. Then, CH sends a packet to all nodes in the cluster. The latter, reply with their IDs and positions. After that, CH compares the received information with its existing table. If IDs and positions

are not unique, the Sybil node is detected from the CH table. The experiments prove that the proposed technique able to detect the Sybil node accurately as well as improve the energy efficiency and the network lifetime compared to [16] and [17].

The most recent technique to detect Sybil attack in cluster topology has been suggested by Priyanka [19]. In this work, the location information is used to detect cluster head which behaves as a malicious node. After selecting a cluster head depending on the level of its residual energy, it will send a packet to the base station which contains its ID and location as well as the ID and location of its members. This process will carry out in each cluster. Then, BS will check if any packet with multiple nodes having the same ID. The process will be repeated to mark the location of the Sybil node by BS. After that, BS will inform the nodes about the location of the Sybil node so that they do not communicate with it. This method works efficiency unless the Sybil nodes send false location information.

3.1.4. RSSI-based Scheme

In [9], Demirbas and Song proposed a method for Sybil attack detection based on the Received Signal Strength Indicator (RSSI) readings of messages. When a node receives a message, it will compute the RSSI of the message and associate it with the sender's ID. Then, when another message with the same RSSI but from a different sender's ID is received, the node can detect the Sybil attack. The analysis results showed that the Sybil attack could be detected with a completeness of 100% with few false positive alerts. Wang et al. [20] proposed a similar RSSI-based scheme in cluster-based WSNs for Sybil attack detection. It establishes the Jakes channel model in which the path loss and fading influence were considered. The experiment results indicate that this method achieves the preferable detection rate.

In the context of clustering-based hierarchical architecture, Jan et al. [21] introduced a received signal strength based scheme to detect the Sybil nodes in WSNs. Their proposed approach requires a collaboration of any two high energy nodes and performs detection using signal strength of received messages. Each node sends messages to its two nearest high energy nodes. The messages contain residual energy and ID of a node. Both high energy nodes compute the signal strength of the received messages and exchange it for computing the RSSI ratio. After a certain period, the same process is performed to compute a new RSSI ratio using signal strength of received messages from the same node. If the new ratio is equal to the previous ratio and IDs of a node in received messages are also different, it means that the node has forged its ID. The results show that the proposed scheme significantly detects the Sybil nodes in comparison with existing methods. Further, RSSI is unstable over the time.

Regarding the stability of RSSI, Marian and Mircea [22] presented a lightweight detection scheme for Sybil attacks based on three nodes collaborations using only their RSSIs without any other computations. The experiments showed that RSSI is stable enough to use it in a security scheme against Sybil attack.

In order to prolong the network lifetime which is affected negatively by Sybil attack, Daiyu et al. [23] put forward a countermeasure against Sybil attack based on RSSI ranging and data flow monitoring. First, they detect suspicious nodes if all of their common neighbors find those nodes have the same distance (by computing RSSI value) to them. Second, a suspicious node will be considered a Sybil node if its data flow is abnormal according to some criterion. Analysis results show that proposed secure mechanism can effectively detect Sybil nodes and extends the network lifetime by 26.3%.

3.1.5. Random Key Pre-distribution

This technique is used to establish secure links between nodes for communicating with each other [24]. In the random key pre-distribution scheme which introduced in [1], a set of keys are assigned randomly to a node enabling it to compute the common keys that it shares with its neighboring nodes. The common keys are used to ensure node to node privacy. The main ideas here are the association of the ID with the key assigned to a node as well as the validation of the key. Validation involves ensuring that the network can validate the key. The fabricated Sybil identity will not pass the test of key validation as the keys associated with a random identity will not likely to have a significant intersection with the compromised key set.

On the basis of the random key pre-distribution scheme, Pietro et al. [25] suggested a pairwise key establishment technique based on the node's identity information to protect the network from the Sybil attack. However, due to the difficulty of building the specific node identity information, the technique is not practical and efficient. Furthermore, Qian presented an improved key pre-distribution mechanism in which each node calculates the derived keys by using a hash function once [26]. This mechanism enhances the security of the original keys. However, the derived keys are calculated by each node after deployment. Therefore, the computational overhead of the nodes is increased.

In order to protect the network against attackers as well as decrease the computational overhead, Bechkit et al. proposed a new hash-based key pre-distribution approach [27]. Before deploying the nodes, a hash function is preloaded to the memory of each node. Then, every node in the network applies the hash function to each key of its key set. After that, the neighboring nodes calculate the pairwise keys using the hash function to establish a secure link. However, in this approach, the calculated pairwise keys are not unique. So, the probability of fabricating the pairwise key by a Sybil attacker is increased. If the

fabricated pairwise key is the same as the legal one, the communication of the neighbor nodes will be disrupted by the Sybil attacker's false identity. In another study, Cheng et al. [5] presented a chain key pre-distribution based approach to defending against Sybil attack. They proposed a lightweight approach to enhance the security of common keys between neighboring nodes. Their approach uses a hash function to create several chain keys by hashing the unique identity information of every node sequentially in the trusted base station. These keys create a pool of chain keys. During the phase of pairwise key authentication establishment, a node-to-node chain key based authentication and exchange (CK-AE) protocol is proposed, by which every node can share the unique pairwise key with its neighboring node. The analysis results show that the proposed approach can not only defend against the Sybil attack but also reduce the communication overhead, which solves the problem in [26].

Regarding cluster-based wireless sensor networks, Archana et al. [28] presented a secure key management scheme adopted on the clustered architecture of WSNs. The proposed mechanism uses partial key pre-distribution in order to identify Sybil attack. Their approach consists of three phases including pre-distribution phase, cluster formation phase, and communication phase. In the pre-distribution phase, each node is loaded with a set of partial keys, an index list of the partial keys, a unique ID and a single network key. In the second phase, after the cluster is formed, the member nodes and CHs send their encrypted IDs to the BS. Then the BS sends the index list to the CHs and their members to find out their partial keys. In the last phase, any two nodes want to communicate with each other, they are verified by their CH if they are within a cluster. Otherwise, they are verified by BS. This solution reduces the load on the BS and the processing time.

3.2. Discussion

Each of the defense mechanisms against the Sybil attack that we have reviewed has different tradeoffs. Most schemes are not capable of defending against Sybil

attack 100%. Additionally, each method has different costs and relies on different assumptions. The radio resource testing mechanism may be breakable with custom radio hardware, and validation may be expensive in terms of energy of nodes. Furthermore, the efficiency of this method depends on the total number of radio channels available to the nodes. On the other hand, the central authority-based methods have larger overheads when applied to large-scale systems. Although this method seems like the ideal solution to tackle Sybil attacks, there are many issues related to the implantation of certification authority specifically about how the CA will establish the entity-identity mapping. In real-world environments, this can be costly if performed manually on large scale systems. Additionally, if the CA is compromised, the whole network falls apart, and all nodes become vulnerable to the Sybil nodes. Position/location verification methods can only put a bound on the number of Sybil nodes generated by an attacker unless they can very precisely verify node positions. Although this method proved its efficiency against Sybil attack, it needs several requirements such as special hardware/software as well as the nodes should be aware of their locations. The biggest problem with this method is that the Sybil nodes may send false location information. The received signal strength indicator based scheme is considered a robust defense mechanism against Sybil attack. In a real-world environment, as the distance between the transmitter and the receiver increases, the strength of the signal becomes weaker. Moreover, the signal strength may be affected by obstructions. On the other hand, the random key pre-distribution scheme has poor scalability as well as adding new node is considered a challenge. Also, the number of keys that must be stored in each node is proportional to the total number of nodes in the network which requires a huge storage space. In addition, establishing of keys via a base station is not secure as base station becomes a target for compromise.

4. Proposed Approach

There are various approaches to detect and prevent Sybil attack in wireless sensor networks as mentioned in the last section. But each of them has its own tradeoffs such as huge storage space, communication overhead, special requirements, etc. Thereby we propose a scheme which can overcome these limitations.

In this section, we describe our proposed scheme to detect the Sybil node which behaves as a cluster head in the wireless sensor network. We first demonstrate the basic proposed scheme, discuss the WSN model and assumptions, and then we describe the algorithm.

4.1. Basic Scheme

Sybil attack poses a threat to clustered sensor network due to the harmful effect on the whole cluster that caused by the Sybil node once it becomes a cluster head. This bad effect degrades security and performance of the network. In response to this problem as well as to overcome the constraints of existing methods, we propose a new defense mechanism to detect the malicious cluster head which has the intention of causing the Sybil attack in WSN.

Our proposed scheme uses the RSSI technique mentioned in [9] to detect Sybil nodes. The detection scheme is based on the fact that any two received messages from the same sender have the same signal strength values which are calculated at the receiver because the sender locates in the same position. In other words, the same RSSI values mean that their associated messages come from same sender (same location). Since the Sybil node may send a message each time with different IDs to the same receiver, the latter can detect the Sybil node by calculating the RSSI value for each message. Then, it will be clear that both RSSIs are the same which means that the message has been received from the same sender but with

different IDs. In this case, there can never be a node with different IDs unless the node is a Sybil node.

Based on this idea, the proposed approach consists of two phases. The first phase includes the formation of clusters as well as suspicion of some nodes may occur at this phase. While the detection of the Sybil node is done at the second phase. In this approach, the base station is considered a central authority which is used to verify the identity of the cluster head to detect the Sybil node according to trust approach in [15].

4.2. Network Model and Assumptions

The clustered sensor network that has been selected consists of N static sensor nodes, including cluster heads, member nodes, Sybil node and a base station. CHs are responsible for collecting the data within their clusters and transmitting it to the BS. The formation of clusters is based on LEACH routing protocol. Every sensor node in the network has a unique identity (ID).

Following assumptions of the WSN are used in the proposed scheme:

1) The proposed scheme will be implemented after deploying the nodes in the network.
2) Sybil node is formed by the compromise of the cluster head.
3) The node with the highest energy will be selected as a cluster head.
4) Each member node joins the cluster head which has the maximum received signal strength.
5) The base station is a trusted device.

4.3. Algorithm

Phase I: (formation of the clusters and suspicion of some nodes)

Step1: The cluster head will be selected among the nodes on the basis of the remaining amount of the energy.

Step2: The Sybil node present in the cluster may steal the identity of the cluster head and broadcast HELLO messages to the nodes asking them to join its cluster.

Step3: The nodes receiving the messages will join the respective cluster heads (including Sybil node) by replying to the message.

Step4: After the election of cluster heads in the network, every cluster head will send a control packet to the BS, which contains the ID of the cluster head as well as the IDs of its members and RSSI values of the received replies from the members.

Step5: The BS will receive the control packets and calculate the RSSI value for each one.

Step6: The BS checks if in any cluster it has a received control packet with multiple nodes having the same ID (here the Sybil node and cluster head have the same ID).

Step7: The ID and RSSI value of both suspects will be stored by the BS in order to detect the malicious cluster head.

The steps of phase I are illustrated in figure 4.3.1.

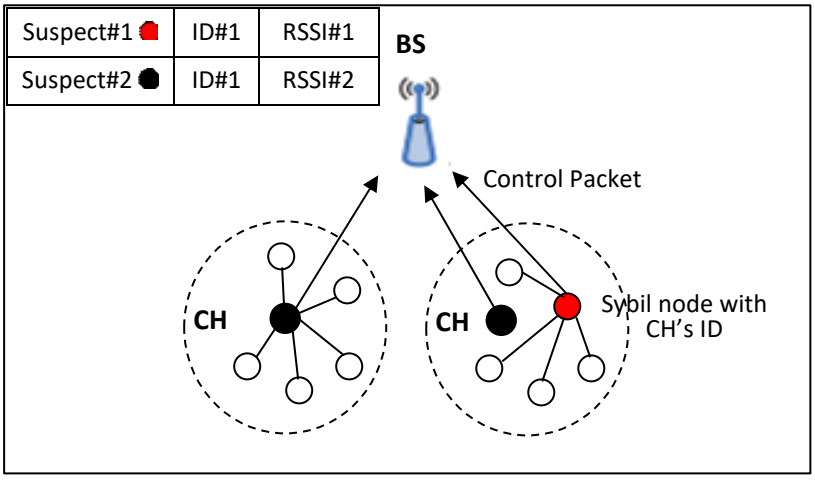

Figure 4.3.1: Phase I (formation of the clusters)

Phase II: (detection of the Sybil node), as illustrated in figure 4.3.2.

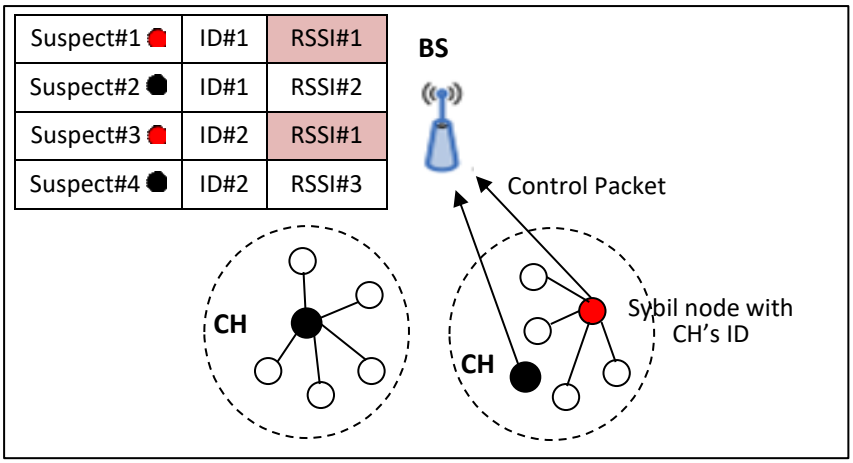

Figure 4.3.2: Phase II (detection of the Sybil node)

Step1: The BS will send a message to the nodes in the suspect cluster to select a cluster head again.

Step2: The Sybil node will again steal the ID of the new cluster head and broadcast HELLO messages to the nodes in the network asking them to join its cluster.

Step3: The nodes receiving the messages will join the cluster head (the Sybil node) by replying to the message.

Step4: The new cluster head will again have to send a control packet to the BS which contains its ID as well as the IDs of its members and RSSI values of the received replies from the members.

Step5: The BS will again receive a packet which contains the same ID for multiple nodes, and it will calculate the signal strength value of the received packet.

Step6: The BS will compare the ID and the RSSI value received in the new control packet with the ID and RSSI value stored previously.

Step7: Since the RSSI values of the messages transmitted by the Sybil node will be the same, the BS will detect that it has received two control packets from two different CHs, but they are located at the same position in the cluster.

Step8: The BS will inform the member nodes in the cluster about the location of the Sybil node so that the nodes do not communicate with it.

Step9: The BS will now elect another cluster head from the list of member nodes received in the control packet.

The proposed approach does not require any special requirements or shared keys to detect the Sybil node. In addition, the base station uses a small memory space to store only the IDs and RSSI values of the suspected nodes. On the other hand, the sensor nodes do not need to be aware of their locations because we can determine their locations using the RSSI technique which helps to save the energy of the nodes.

5. Conclusion

Nowadays, the Sybil attack is a major problem that suffers the wireless sensor network badly. There are various approaches to detect and prevent Sybil attack in such network. However, each of these techniques has its own tradeoffs and not suitable for the limited resources of the sensor nodes. Therefore, an efficient scheme is required to detect Sybil attack without additional overhead as well as to conserve energy and prolong the network lifetime.

In this paper, we proposed a defense mechanism against Sybil attack, which can overcome the limitations of existing approaches. Our solution can detect the Sybil node which behaves as a cluster head in a clustering-based hierarchical network. The method is based on the RSSI technique to determine the location of the nodes without any additional requirements. Also, we used the trust concept to make the base station a central authority which is used to verify the identity of the cluster head in order to detect the Sybil node. The proposed approach consists of two phases. The first phase includes the formation of clusters as well as suspicion of

the nodes that have abnormal behavior. While the detection of the Sybil node is performed at the second phase.

In the future, we plan to improve our Sybil attack detection scheme in WSNs by taking into account that the Sybil node may be a strong enough to be able to alter the RSSI values. Therefore, we have to address this situation and prevent Sybil nodes from any alterations.

REFERENCES

[1] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," *Proceedings of the third international symposium on Information processing in sensor networks IPSN04*, pp. 259–268, 2004.

[2] J. R. Douceur, "The Sybil Attack," pp. 251–260, 2002.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, 2003.

[4] D. Mukhopadhyay and I. Saha, "Location verification based defense against Sybil attack in sensor networks," in *International Conference on Distributed Computing and Networking*, 2006, pp. 509–521.

[5] C. Cheng, Y. Qian, and D. Zhang, "An approach based on chain key predistribution against Sybil attack in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 11, 2013.

[6] R. Singh, J. Singh, and R. Singh, "TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks," *International Journal of Computer Science and Network Security*, vol. 16, no. 11, pp. 90–99, 2016.

[7] S. Kaur and R. Naaz Mir, "Clustering in Wireless Sensor Networks- A Survey," *International Journal of Computer Network and Information Security*, vol. 8, no. 6, pp. 38–51, 2016.

[8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 2000, vol. vol.1, p. 10.

[9] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, p. 5, 2006.

[10] A. M. Bhise and S. D. Kamble, "Review on Detection and Mitigation of Sybil Attack in the Network," *Procedia Computer Science*, vol. 78, pp. 395–401, 2016.

[11] N. Balachandran and S. Sanyal, "A Review of Techniques to Mitigate Sybil Attacks," *International Journal Advanced Networking and Applications*, pp. 1–6, 2012.

[12] S. Sharmila and G. Umamaheswari, "Detection of Sybil Attack in Mobile Wireless Sensor Networks," *International Journal of Engineering Science & Advanced Technology*, vol. 132, no. 2, pp. 256–262, 2012.

[13] S. Sinha, A. Paul, and S. Pal, "The Sybil Attack in Mobile Adhoc Network: Analysis and Detection," in *Third International Conference on Computational Intelligence and Information Technology*, 2013, pp. 458–466.

[14] H. N. Saha, D. Bhattacharyya, and P. K. Banerjee, "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack," *International Journal of Computer Science & Emerging Technologies*, vol. 1, no. 4, pp. 338–341, 2010.

[15] H. Singh, R. Singh, and J. Singh, "Protecting Cluster Head from Sybil Attack in Wireless

Sensor Networks," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, 2017.

[16] P. R. Vamsi and K. Kant, "A lightweight Sybil attack detection framework for Wireless Sensor Networks," in *Seventh International Conference on Contemporary Computing (IC3)*, 2014, pp. 387–393.

[17] K. F. Ssu, W. T. Wang, and W. C. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.

[18] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, and A.-S. K. Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks," in *3rd International Conference on Eco-friendly Computing and Communication Systems*, 2014, pp. 95–98.

[19] Priyanka, "Efficient Defense Mechanism against Sybil Attack in Wireless Sensor Network," *International Journal of Engineering and Computer Science*, vol. 6, no. 5, pp. 21465–21467, 2017.

[20] J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," 2007, no. 6, pp. 2684–2687.

[21] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil attack detection scheme for a centralized clustering-based hierarchical network," *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 318–325, 2015.

[22] S. Marian and P. Mircea, "Sybil attack type detection in Wireless Sensor networks based on received signal strength indicator detection scheme," *SACI 2015 - 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, pp. 121–124, 2015.

[23] D. Xu, Y. Wu, and Y. Duan, "Sybil Attack Detection Scheme Based on Data Flow Monitoring and RSSI ranging in WSN," in *2nd International Conference on Mechatronics and Information Technology*, 2017, pp. 110–114.

[24] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," 2003, pp. 42–51.

[25] R. Di Pietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure Wireless Sensor Networks," *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks - SASN '03*, p. 62, 2003.

[26] S. Qian, "A Novel Key Pre-distribution for Wireless Sensor Networks," in *International Conference on Solid State Devices and Materials Science*, 2012, vol. 25, pp. 2183–2189.

[27] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new class of Hash-Chain based key pre-distribution schemes for WSN," *Computer Communications*, vol. 36, no. 3, pp. 243–255, 2013.

[28] M. B. Archana, B. N. Harshitha, and M. Prajakta, "A technique to safeguard cluster-based Wireless Sensor Networks against Sybil Attack," *International Journal of Recent Trends in Engineering & Research*, vol. 3, no. 4, pp. 370–373, 2017.