Detecting Node Masquerade Attack using RLE Method

Rimple Manni and Lavish Kansal*

School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India; rimple.713@gmail.com, lavish.15911@lpu.co.in

Abstract

Among security challenges raised by mobile Wireless Sensor Networks, clone attack is particularly dreadful since it makes an adversary able to subvert the behavior of a network just leveraging a few replicas of some previously compromised sensors. In this work, we propose a method named as Detecting Node Masquerade Attack using RLE Method which is used for detecting a clone in the network using RLE method. The main goal of our proposed protocol is to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as RSSI and List Exchange method i.e. R represents RSSI means received signal strength indicator. After that we also compare our proposed protocol with the known method i.e. Hip-Hop protocols which are also used to find a clone in mobile WSN and our simulation shows that our proposed protocol outperforms the existing approach in terms of detection rate and time taken to detect a clone. In future work, we can also use a clustering protocol to make this work more efficient.

Keywords: Reprogramming, Security, Sensor Networks

1. Introduction

Wireless Sensor Network (WSN) is a form of network that consists of a large number of sensors which are very small in size and less costly. With the help of recent advancements in wireless communication and technologies, these sensor nodes can be able to sense environment information, process the gathered data and also deliver that information to the main base station via different wireless channels1, 2. Main applications of sensor networks are data gathering processes such as environmental monitoring, Body area networks, military services etc. These sensors send data either in periodic manner or in the event wise according to the desired application. In this work, we focus on the security of WSN, security is related to authentication, privacy and integration of data in the wireless systems3,4. Mainly, we deal with the clone attacks in this in which replica of different nodes is present in the system and which create security issues in the network.

2. Present Research Scenario

Wireless Sensor Network is a network of sensor nodes without having any central controller. Its growth is increasing day by day and that’s why there is a wide field for research in this area. In the base paper, they described about the detection of the presence of cloned nodes in a mobile WSN and they have proposed two protocols using Hip-Hop protocols5. But there are many loopholes in those protocols i.e. if the clone nodes are distributed in whole network. It cannot be detected by either hip or hop protocol6. For the detection of clone in the hop protocol it necessary to have common node for the detection of clone. So in both cases the clone cannot be detected at the initial stage7. The opponent can do any with network (network jamming, steal secure information). The major challenges in WSN are like security and some security mechanism to improve the safety of the network. Basically, they describe about all the security attacks in
 Detecting Node Masquerade Attack using RLE Method

the Wireless Sensor Networks and with their threats and also security in WSN is an important factor to get acceptance and use of sensor networks\(^8\). Basically in mobile sensor networks, the detection of the clone is done by the various centralized and distributed protocols in the static and mobile environments. Some of the protocols are RED, BC-MEM and P-MPC. Randomized, Efficient and Distributed (RED) protocol for the detection of node replication attacks\(^9,10\). They have introduced the preliminary notion of ID obliviousness and area-obliviousness that convey a measure of the quality of the node replicas detection protocol; that is, its resilience to a smart opponent. At the end, they compare the RED protocol with the state-of-art (LSM) and proved that overhead by RED are low as compared to others.

There are also some previous techniques of clone detection that if clone is distributed in the whole network it cannot be easily detected. So, there are different methodology of detecting clone i.e. Randomized Multicast distributes node location information to randomly selected witnesses, exploiting the birthday paradox to detect replicated nodes, While Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection and Line-Selected Multicast displays particularly strong performance characteristics\(^11,12\). Finally, the result shows that Line-selected Multicast shows better performance. They described the clone attacks in the mobile WSN and there are many ways to tackle a clone attack but they usually suffer from high overhead. There is also a new method i.e. MACDC method which is used to detect replica using mobile technology and results prove that this method is better than the other known solutions in terms of the energy consumption and overhead of the network. At the time of routing, there is also possibility of insecure network\(^13\). For this many solutions has been proposed like they have proposed a routing algorithm but as its not simple routing algorithm although they have proposed a secure routing algorithm in WSN and they introduces two categories of novel attacks against sensor networks that is sink holes and hello floods and examine the security of all sensor networks\(^14,15\).

Our proposed algorithm, this protocol works in two parts and the main goal of our proposed protocol is to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as R represents RSSI (Received Signal Strength Indicator), L represents location of the nodes in the network and E is for energy of the nodes in the network. In the part 1, the nodes in the following network make clusters or groups and in the other part, detection of the replica nodes is being done by using RLE method. This protocol improves the limitations of the base paper and our simulations shows that proposed work outperforms the base protocols in terms of parameters like detection rate and time taken to detect the clone.

3. System Model (Detecting Node Masquerade Attack using RLE Method)

The main goal of our proposed Detecting Node Masquerade Attack using RLE Method which is used to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as R represents RSSI (Received Signal Strength Indicator), LE represents list exchange in the network. This protocol works in two parts. In the part 1, the nodes in the following network make clusters or groups and in the other part, detection of the replica nodes is being done by using RLE method.

3.1 Part 1: Cluster Formation and CH Election

Whenever there is deployment of the nodes in the network, firstly the whole network is divided into the clusters and after that each cluster in the network will go for CH election process in which the nodes which are near to the Base station will became leader or CH (Cluster Head) that means CH election is based upon the distance because the less distanced node will stay for more lifespan in the network and after this part detection process started.

3.2 Part 2: Detection of Clones using RLE Method

In this part, firstly CH gathered all the information from each node within their cluster and this information includes RSSI value and exchange the member list with their unique ID. Now, each CH within their respective cluster chooses the two nodes with their smallest RSSI values and unique ID and send these gathered information to the BS. The work of comparison of all these values is being done by BS as it have all the information of ID and smallest RSSI values of nodes from CH. Now, on the
basis of comparison of unique ID of nodes, BS will find the clone node because two nodes cannot have the same unique id and after this BS will compare the RSSI values of the same suspected nodes.

4. Simulation Setup

At the end, we evaluate the performance of our proposed algorithm to other well-known our base algorithm i.e. Hip-Hop protocol. Mainly, the performance of the algorithm will be evaluated on the basis of following metrics: (1) Detection rate, (2) Detection time. The simulation is being done in Mat lab MATLAB is a programming language developed by Math Works. It started out as a matrix programming language where linear algebra programming was simple. Initially deployment of all the sensor nodes is done in 100 X 100. Here the number of sensor nodes is 500. After that the whole network was divided into clusters and the deployment of the base station occurs in the center of the network.

There are two parameters to check the performance of the network i.e. Detection rate and Detection time:

- **Detection rate.** The inverse of the ratio between the total number of nodes that has heard of the malicious node and the number of those that considers it as suspicious. Higher the detection rate better will be the network will be.
- **Detection time.** It shows how much time a system takes to detect the suspicious nodes.

In the simulation scenario, the Figure 1 represents, the detection rate of hop protocol approx. 0.6 and using RLE method it becomes equal to 1 and simultaneously, Figure 2 represents the detection time of hop protocol approx. 3.4 and using RLE method it becomes equal to 2. In other words, we can say that the detection rate of Hip-Hop protocol is approximately 60% and using RLE method it becomes equal to 100% and also, the detection time of Hop protocol approximately 3.4 seconds and using RLE method then it becomes equal to 2 seconds. The results declared in this part clearly show that our proposed Detecting Node Masquerade Attack using RLE Method is more efficient and reliable than base algorithm in all considered scenarios in terms of Detection rate and Detection time as well.

5. Conclusion

In this work, we proposed a new proposed method i.e. Received Signal Strength Indicator (RSSI) and List Exchange method by which out Detection rate and time taken to detect clone has been changed. In the comparison of results with the previous approach, the Detection rate of Hip-Hop protocol is approximately 60% and using RLE method it becomes equal to 100% and also, the detection time of Hop protocol approximately 3.4 seconds and using RLE method then it becomes equal to 2 seconds. In the future work, we can also use clustering approach to save the energy of the nodes because in WSN,
the nodes are based on battery level so conserving battery life is the major issue and we can use many clustering protocols to make the clusters of the nodes to increase the lifetime of the nodes and hence overall network lifetime will improve.

6. References