Secure and Efficient Detection of Replica Node Attacks by Using Fast Randomized Algorithm in Wireless Sensor Network

Karthikayine.D¹ UdhayaShankar.S.M²
Student¹, Faculty², Department of IT, Velammal Engineering College, Anna University, Chennai, India
Email: karthikayine91@gmail.com¹/ udhaya3@gmail.com²

ABSTRACT

The emerging Wireless Sensor Network (WSN) technology has many security issues due to its unattended nature. Node Replication Attack is a kind of application independent attack in which an adversary deploys its own inexpensive sensor nodes in the network as legitimate sensor nodes. In the existing system, using Localization Algorithm is to resist node replication attacks in mobile sensor networks. Localized algorithm includes localized detection, network-wide synchronization avoidance and network-wide revocation avoidance. Less performance comparisons with known methods are provided to demonstrate the efficiency of our proposed algorithms. In the proposed system, using fast randomized algorithm to identify the genuine node ID available in the network or not, which is verified and compared with the requested node ID to detect whether it is Replica or Genuine node ID. Here, Server maintaining each and every requested node ID’s for data transmission. Further Server will monitor the location of the network ID, Node ID and Node Password for the secure communication of the entire networks. In the Modification, Primary Key will be changed on Random basis with Time Stamp and also whenever attack occurs. Source node will specify Time to Live (TTL) for every data transmission, based on the TTL value priority of the packet is identified and transmitted accordingly.

Keywords:
Wireless sensor networks security, node replication attack detection, distributed protocol, resilience, efficiency

1 INTRODUCTION

Mobile wireless sensor networks (MWSNs) can simply be defined as a wireless sensor network (WSN) in which the sensor nodes are mobile. MWSNs are a smaller, emerging field of research in contrast to their well-established predecessor.
MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. A wireless sensor network (WSN) consists of a number of tiny, low-cost, and resource- constrained sensor nodes, but is often deployed in unattended and harsh environments to perform various monitoring tasks. As a result, WSNs are susceptible to many kinds of threats and attacks. While most of them are dealt with through cryptographic materials provided by the management protocols, some other threats like node replication attacks are one of the most redoubtable attacks where an attacker compromising a node uses its secret cryptographic key materials to successfully populate the network with clones of it.

2 NODE REPlication ATTACKS

The node replication attack, an adversary captures a node physically and reproduces the node using the secret credentials which has been extracted and deploys them in the network and disables the Wireless Sensor Network applications. It affects a wide variety of applications such as object tracking to battle surveillance because of its application independent nature. It is also known as clone attack wand the static and mobile wireless sensor networks, the security issues are the same.

It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member.

It creates various attacks by extracting all the secret credentials of the captured node. It corrupts the monitoring operations by injecting false data. It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too.

To instigate this attack, an adversary only needs to physically capture one node, and after collecting all secret credentials (ID, cryptographic keys, etc.), an adversary replicates the sensor node and deploys one or more clones of the compromised node into the network at strategic positions, damaging the whole network by carrying out many internal attacks.

3 RELATED WORKS

Various techniques have been proposed for detection node replication attacks in mobile sensor networks in which some of them are distributed detection algorithms and centralized detection algorithms. The localized algorithm is a particular type of distributed detection algorithm. Some of the techniques that are found for detecting and preventing node replication attacks are summarized.

3.1 RANDOM KEY PRE-DISTRIBUTION

Key establishment is an emerging problem in nodes in mobile sensor network. The nodes are compromised by an adversary. There are three mechanisms proposed[1]. The first mechanism is Q-composite scheme.
The Q-composite scheme in which a key must be selected from the key ring by two nodes. The Q-composite scheme enhances security in small scale networks at a cost with greater susceptibility. The multipath reinforcement scheme improves security at a cost of network communication overhead. It has the best properties with the variation in node deployment density which is low. The random pair wise schemes has better security against node capture and prevention of node replication of nodes. The witness finding strategy is the technique used in random pre distribution which helps in finding the lowest communication range. The Q-composite scheme differs in the pool size while compared with the basic scheme. The random pair wise does not need the key to be stored in the key’s ring. It has two phases: pre-deployment initialization and post deployment setup phases. The three schemes are used for solving the security bootstrapping problem in the nodes which are resource constrained.

3.2 RANDOM WAY POINT MODEL

The random way point model is used for efficient communication in sensor networks which can be implemented in simulation tools like ns-2 and GloMoSim and also used in adhoc networking protocols. The random way point model determines the stochastic properties and the movement of each node. Each node calculates the destination node and the speed it has to travel to reach the destination. The time taken by the node to travel from starting position to destination node is called the transition. The two major parameters are speed behavior and direction change behavior. The random way point model are uniformly distributed per definition. The derived direction distribution determined that the nodes move back to the middle of the area.

3.3 EFFICIENT AND DISTRIBUTED DETECTION

The Efficient and Distributed Detection and its variant Storage Efficient and Distributed scheme are possessed with properties like distributed detection, efficiency, effectiveness. The efficient and distributed detection scheme can be learnt from the two observations with and without replicas[4]. In a network without replicas the number of times the node encountering a specific node must be within the limited interval of specified length with high probability whereas in a network with replicas the number of times a node encountering a specific which must be greater than the threshold with specified length. The Storage Efficient Distributed Detection varies from Efficient Distributed Detection that it monitors only a set of nodes which can be called as monitor set. The two factors are communication range and length of sensor nodes.
3.4 STATISTICAL EN-ROUTE FILTERING

In a large scale network, the nodes are compromised and added in the network and if they are not detected then it would be forwarded to the sink. It causes attack which implies loss of power and bogus alarms. To prevent this, a mechanism called Statistical En route filtering mechanism is used[4]. It possess Multiple keyed message authentication codes that provides security which generated by each node.

This mechanism detects and drops bogus reports which is a greater advantage. The collective decision-making and collective false-report detection by multiple detecting and forwarding nodes respectively for the purpose of determining the truthfulness of each report. The Centre Of Stimulus(CoS) is responsible for collecting all data and produce reports which is send to the sink. It has a global key pool and three components[2]. They are sink, report and intermediate nodes. The sink verifies the MAC for the report it receives. The disadvantage of Statistical En Route Filtering is that it can’t detect and drop many compromised nodes at once in a large scale network.

4 SYSTEM ORGANIZATION

The network consists of ‘n’ number of nodes. The nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. Server is the module which is used to store all the nodes information like Node Id, Password. Also the Server will monitor all the node’s communication for security purpose. Each node will be having primary key for security purpose. Source node also specifies TTL (time to live). TTL is based on priority. There are three types of priority that is high, medium, low priority.

For example If the source node spends < 5sec to send data means server gives high priority. At the same cycle another source node spends 5-10sec to send data means it gives medium priority. Similarly another source node spends > 10sec it gives low priority. Server verifies Source node’s information like User ID, Password and along with the Primary Key. If the primary key is correct means only, the server will allow to transfer the packet to the destination. This primary would be altered with respect to Time Stamp on random basis which is updated to the corresponding node continuously. Primary key is changed on two occasions; one is on the random basis and another when the attack occurs. When the replica node sends a data to the server, Server verifies its ID, Location and Primary Key. Server will be verifying the User Specified ID on the GUI with the Original ID Specified in the packet Header. If those two ID’s are varying then the Primary Key of that genuine node will be altered. Finally server checks the each node energy level after data transmission using prediction algorithm. Prediction algorithm is used to fix the energy level of each node. And it also checks the node energy for before and after data transmission.
After detection of energy, server reassigns the node energy based on node reliability using new routing algorithm.

When the replica node sends a Data to the server, Server verifies its ID, Location and Primary Key. Server will be verifying the User Specified ID on the GUI with the Original ID Specified in the packet Header. If those two ID’s are varying then the Primary Key of that genuine node will be altered.

### 4.2 RANDOMIZED NETWORK LOCATION OF NODE AND DATA TRANSMISSION

This module is used to identify the current location of node. Source node transmits data to destination node via intermediate node using signcryption algorithm. Before data transmission server checks the source node energy level using prediction algorithm. Signcryption is a technique of performing signature and encryption in a single logical step. It is a secure and efficient technique of providing security between the sender and the receiver. Source node primary key verified by server to reach destination using fast randomized algorithm.

### 4.3 PRIMARY KEY AND AUTHENTICATION

Server verifies Source node’s information like User ID, Password and along with the Primary Key. This primary would be altered with respect to Time Stamp on random basis which is updated to the corresponding node continuously.

Primary key is changed on two occasions; one is on the random basis as discussed above and another when the attack occurs.
4.4 TTL BASED ON PRIORITY

In this concept source will specifying the TTL (Time To Live) for the data transmission. TTL is based priority. In the project these maintain three types of priority that is high, medium, low priority. For example if the source node spends < 5sec to send data means server gives high priority. At the same cycle another source node spends 5-10sec to send data means it gives medium priority. Similarly another source node spends > 10sec it gives low priority.

4.5 RECYCLING PROCESS BASED ON ENERGY LEVEL

In this module, server checks the each node energy level after data transmission using prediction algorithm. Prediction algorithm is used to fix the energy level of each node. And it also checks the node energy for before and after data transmission. After detection of energy, server reassigns the node energy based on node reliability using new routing algorithm.

5 FAST RANDOMIZED ALGORITHM

The Fast Randomized Algorithm to identify the genuine node ID is available in the network or not, which is verified and compared with the requested node ID to detect whether it is replica or genuine node ID. If the node ID is same then it is a genuine node. Else it is a replica node and it is blocked from accessing the network. This is an algorithm which gives excellent results when detecting and verifying on both source location as well as destination location via the server in the networks and is much faster, typically thousands of times faster, than localized algorithms. It gives a new randomized algorithm for achieving consensus among asynchronous processes that communicate by monitoring for every node in the entire network.

6 CONCLUSION

The Fast randomized algorithm is used to identify whether the genuine node ID is available in the network or not and which is compared and verified with the requested node ID. Hence the probability of malicious node is reduced. The primary key is monitored for every node; this primary key will be changed on random basis with time stamp and also when an attack occurs. So the efficiency of the security is enhanced. Source node will specify Time To Live (TTL) for every data transmission, based on the TTL value priority of the packet is identified and transmitted accordingly. Hence the data can be send securely based on the priority that is assigned through TTL.
REFERENCES


