IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sep-Oct. 2014), PP 65-70
www.iosrjournals.org

Node Replication Attack Detection Algorithms in Wireless Sensor Networks: A Survey.

Mayur R. Khandekar[1], Prof. U. K. Raut[2]
[1](Department of Computer Engineering, Maharashtra Institute of Technology, Pune, India)
[2](Department of Computer Engineering, Maharashtra Institute of Technology, Pune, India)

Abstract: *The sensor networks are often deployed in hostile environments and are not attended for long time. Deployment of these networks is increased in the recent years, as they help in monitoring and analyzing different properties of the environment. The application of wireless sensor network starts from environment, household monitoring and ranging up to critical military applications. The sensor nodes in the network are prone to different kinds of novel attacks. An attacker, with little effort, may physically capture nodes, exploits the information on the node, reprogram the node and create replicas, and secretly insert these replicas at strategic locations within the network. This is called as node replication attack. Since these replicas have legitimate access to the network (legitimate IDs, keys, other security credentials, etc.), they can participate in the network operations in the same way as a legitimate node, and thus a large variety of insider attacks takes over the network. Using such nodes the attacker can corrupt the data flowing through the network, also the attacker can disconnect some part of the network with other part of the network. Detection of node replication attack is therefore important. So, in this report we will come to know about some node replication detection schemes, out of which some depend primarily on centralized mechanisms where the base station plays very important role, and others depend on distributed detection schemes. The detection probabilities and communication overhead are the major concern while proposing and using the detection techniques. Hence, the design of efficient algorithm to detect node identity replicas is still an open and demanding issue.*

Keywords: *Wireless sensor network, Replication attack, Centralized Detection schemes, Distributed Detection schemes, Security.*

I. Introduction

Wireless sensor network (WSN) consist few to several hundreds or even thousands of specially distributed, small in size and inexpensive nodes which monitors assets of environment such as temperature, sound, pressure etc. The acquired data is wirelessly transferred through the network to the main system, also called as base station or host system. The data can be collected, processed, analysed at host system. The development of wireless sensor networks was motivated by military applications, and today such networks are many industrial and consumer applications [2][1].

These WSN networks are prone to different type of attack like network intrusion attacks, routing attacks, identity attacks [1]. In many cases nodes are deployed in danger areas, where we cannot go often. In this type of sensor network the attacker can physically capture the node and can make as many replicas and deploy them in the network. This nodes have the same node ID's. The attack is called as node replication attack, it is one of the identity attacks. These replicated nodes have legitimate access to the network like all the other nodes in the network. So these replicated nodes can take part in all the activities of the network, which can result in many different types of insider attack. If these clone nodes are not detected, it will harm the network. So detection of such nodes is very important.

This paper surveys different algorithms to detect node replication attack in WSN, classification of algorithm, limitation of algorithms. The rest of the article is organized in the following way: Section II gives some information about node replication and classification of detection algorithms. Section III tells about the centralized detection schemes Section IV gives the information about distributed detection schemes. Section V concludes the paper.

II. Node Replication Attack

In node replication attacks, first the attacker physically captures the node and exploits the information on the node in a certain amount of time, reprogram the sensor node, and then place that node again inside the network. Then the attacker creates many replicas of the captured node and places those nodes in the network. By using these nodes the attacker can make different types of attack on the network. After compromising the node, the attacker exploits the confidential information, including secret keys and uploads it on other replicated nodes. Other nodes in the network assume them as legitimate nodes, as they have valid credentials. So these clone nodes can communicate with the other nodes in the network.

To detect the replicated nodes, different algorithms are developed. These algorithms are developed for network those are having stationary sensor nodes, the nodes are not mobile. Depending on the working behaviour of algorithms, they are classified into two schemes, Centralized detection schemes and distributed detection schemes.

The centralized detection schemes are dependent on the base station, the base station collects data from the sensor nodes present in the network. Base station also helps in executing replica detection algorithm. This base station plays very important role in centralized detection schemes. The nodes inside the network transfers the node ID's and location claims (LC) to the base station, and base station do the main work of identifying the replicas inside the network. After identifying the replicated node or clone node, the base station broadcasts the revocation message inside whole network. As the whole process is done by base station, it is called as centralized detection scheme.

The distributed node replica detection schemes are not dependent on the base station for their working, but the nodes inside the network itself execute the algorithm and detect the replicated nodes, as these algorithms are executed on distinct nodes of the WSN, they are called as distributed detection schemes, the distributed detection schemes are preferred over the centralized detection schemes due to some demerits in the centralized schemes which we will see in later part of report.

III. Centralized Detection Schemes

This section gives information about some basic and recent centralized detection schemes that are used to detect the replicated nodes inside the network.

3.1 Straightforward scheme.

As shown in Fig. 1 in Straightforward schemes [4][5] nodes a1 and node b1 are replicated nodes. According to the straightforward schemes, node A and node B will send node ID's and location claims of their neighbors to the base station, i.e. node A will send information about node a1 and node a2 to the base station and node B will send information about node b1 and node b2 to the base station. Now after getting all the node ID's and location claims, the base station compare the ID and LC of each node with the ID and LC of all other nodes that are inside the network, the BS finds node a1 and node b1 are having same ID but different LC. The BS will revoke the clone nodes by flooding the network with an authenticated revocation message.

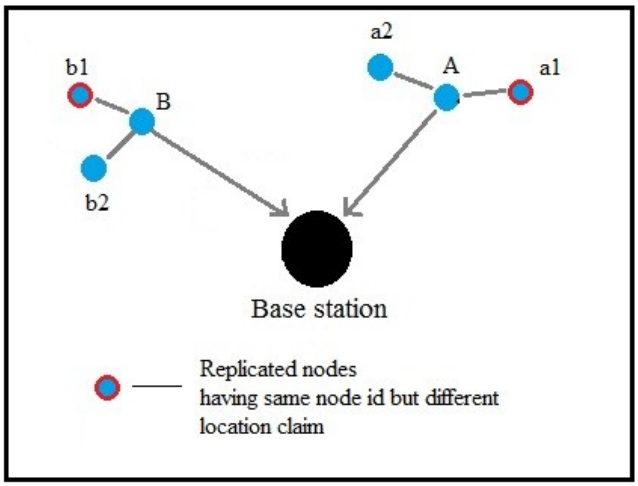

Fig 1 : StraightForward Scheme

The main disadvantage of this method is that all the nodes has to transfer location of their neighbors to the base station, which increases the traffic in the network, again many redundant messages with same ID and LC will arrive at base station. So, the communication cost of this method is very high.

3.2 SET operation.

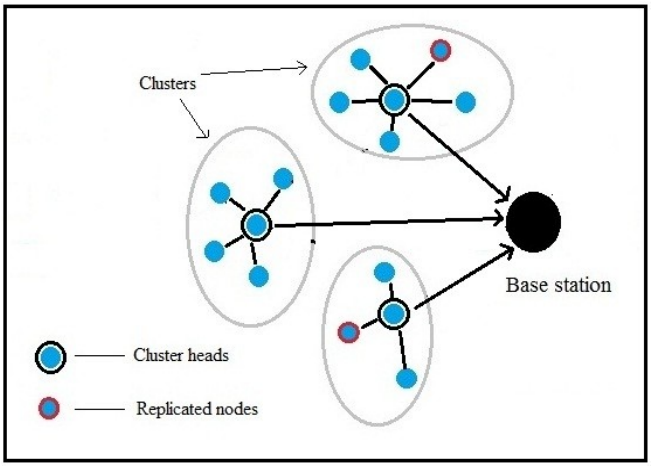

Fig. 2 Set Operation

Another centralized detection technique known as SET proposed in [6]. This algorithm partitions the network into regions (clusters), every cluster has one cluster head, this cluster heads takes the ID's of all nodes inside the cluster and passes all ID's to the base station along with its own ID in the form of subset. The intersection operation is performed on all these subsets. The intersection of any two subsets should be empty, otherwise a clone is detected. Then revocation of such node is done.

3.3 Detecting Cloned Keys.

A clone detection protocol based on random pairwise key pre-distribution scheme is proposed in [7]. This clone detection protocol uses random pairwise key pre-distribution scheme. This protocol finds the clone present inside the network by analyzing the node authentication statistics. A counting Bloom filter is used for collecting key usage statistics. The nodes use these keys to set up a connection with each other, also for encrypting and decrypting the data. But this protocol only considers the key usage for authentication purpose. When the clone nodes are inserted into the network, the key usage is skewed. The cloned keys are present on greater number of nodes than normal, implying that they are used more frequently compared to other keys that are not cloned. So by collecting key usage statistics, it can be found that which key is used more than a certain threshold value. These keys are considered as cloned keys and are erased from the network.

3.4 Area Based Approach for Node Replica Detection.

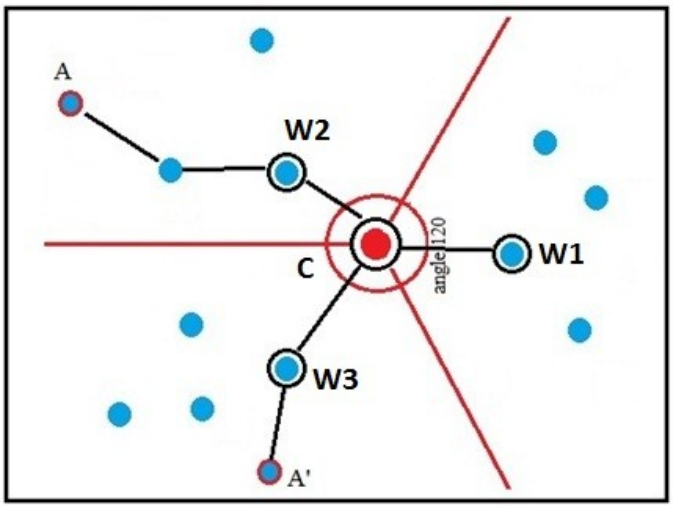

Fig. 3 Area based approach for node replication detction

This [5] approach attempts to combine the advantages of centralized and clustering approach. First the Centre node(C) is selected based on the maximum neighbor nodes approach. The maximum neighbor approach finds the node having maximum number of neighbor and considers that node as the center node. Then the area around the center node is divided into sub-areas equally based on the angle made on center node. A Witness node (W) is assigned to each sub area.

The process of ABCD method can be also illustrated in Fig. 3. Let node A be the original node and A' be the replicated node, these two nodes are in two different sub areas. Node A sends its node ID and location claim to its neighbor. Then, its neighbors sends ID and location claim of node A to a witness node W2, this ID and location claim are passed through the intermediate nodes to the witness node. Similarly A' will send its location claim to its witness node. The replica detection is done at the center node, when two different location claim conflicts for the same node ID. Then the center node broadcasts the conflicting detection message to all nodes in the network.

3.5 Demerits of Centralized Detection Scheme.

Centralized detection schemes have higher detection rate, but as they are having certain demerits, they are not mostly used for replica detection. These algorithms are having demerits like single point of failure, as these schemes rely on base station for detection purpose. If base station is gets down then the algorithm also fails. Another demerit is that the nodes that are near the base station exhausts very quickly compared to other nodes, as all the location claim and ID are passed through these nodes to the base station. Another issue is that the base station cannot start executing the algorithm till it will not get location claim and ID of all the nodes, some good amount of time is required for collection this information, so it is a time consuming process. Also many networks do not have powerful base station to collect all this information, analyses this information, identify the conflict and perform the revocation action. So the base station becomes the important factor.

IV. Distributed Detection Schemes

Another approach for detecting the replicated nodes inside the sensor network is distributed detection schemes. Following are some distributed detection method proposed by researchers. These node replica detection schemes do not rely on the base station for their working.

4.1 Node to Network Broadcast.

In Node to Network Broadcast [4] every node present in the network broadcasts its own location claim and node ID to all the other nodes in the network. Every node also stores the location claim and node ID of its neighbour. The algorithm runs on every node of network. Every node compares the ID and location claim it receives with the location claim and ID of its neighbours. If it finds a conflicting location claim for same ID then it broadcasts a revocation message.

This protocol achieves 100 % detection of replicated nodes, if every node receives the broadcasted node ID and location claim. But, this protocol requires each node to store information about all its neighbours and also need to store the broadcasted message. So the communication cost in this algorithm is very high. For large networks it is very costly.

4.2 Deterministic Multicast.

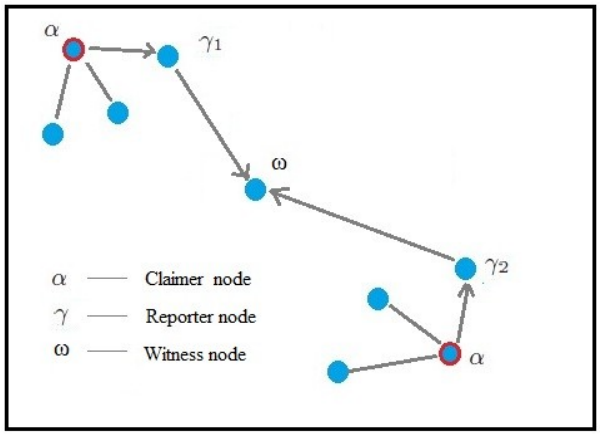

Fig. 4 Deterministic Multicast

The DM protocol [4] follows the claimer-reporter-witness framework. In the previous method the node pass its location claim to all other nodes in the network. This overload is reduced in this this algorithm. The location claim and ID's are passed to limited no of deterministically chosen witnesses. The claimer node claims for a particular geographical location.

The claimer node locally broadcast its location claim to its neighbor, these neighbor serve as a reporter. The reporter chooses the witness node as a function of node ID. Then the reporter passes this location claim to witnesses. If a node is replicated in the network then the witness will receive conflicting location claim for same node ID. Problem in this algorithm is that the selection of witnesses is deterministic, as the function is

deterministic. The attacker can determine the witness node and can compromise that node before inserting the clone node inside the network. So the algorithm will not be able to detect clone node.

4.3 Randomize Multicast.

This algorithm in [4] is extension of the Deterministic Multicast. The witnesses are not chosen by mapping the node ID to function, but they are randomly chosen by algorithm, so it will be difficult for the attacker to identify the witness for particular node ID. When the claim claims for location, each of its neighbors which serve as reporter transfers this location claim to randomly chosen witnesses. If there are n nodes inside the network and location produces square root of n witnesses, the according to the birthday paradox at least one node will receive conflicting location claim.

4.4 Line Selected Multicast (LSM).

Another method given in [4] is developed for detecting the clone node and which also reduces the communication cost of the previous algorithm to some noticeable value. Line Selected Multicast is the improvement to Randomize multicast. When the reporter nodes send the location claim to the randomly selected witnesses, the nodes in the path also stores the copy of location claim. The intermediate nodes check the location claim with the other claims in its buffer for conflict, and then forward the claim ahead. So the conflicting claims can be identified on the intermediate nodes only, we don't have to move further. That reduces the communication cost.

4.5 Random Efficient and Distributed Protocol (RED).

This protocol executes at fixed time intervals [10][9]. It is executed in two phases. In first phase a random value, *rand*, is broadcasted to every node of the network. In the second phase each node sends its claim to neighbours, and then neighbour sends this claim to pseudo-randomly selected witnesses. The pseudo random function takes the *rand* value to select the witnesses, this makes it difficult for the attacker to detect the witnesses and so he cannot compromise the witnesses. The witness's changes after every iteration of the protocol as the *rand* value changes for every iteration. Conti et al. has given the following algorithm in [10].

Algorithm: RED

1: **Procedure** BROADCAST_CLAIM
2: *claim* → < ID_a, is_claim, location(), time() >
3: *signed_claim* ← < *claim*, K_a^{priv}*(claim)* >
4: a →neighbors(): < ID_a, neighbors(), *signed_claim* >
5: **end procedure**
6: **Procedure** RECEIVE_MESSAGE (m)
7: **if** is_claim(*m*) **then**
8: < - , - , *signed claim* > ← *m*
9: < *claim, signature* > ← *signed_claim*
10: **if** bad_signature(*claim, signature*) **then**
11: discard *m*
12: **else if** incoherent_location(*claim*) **then**
13: < ID_x, - , - , - > ← *claim*
14: trigger revocation procedure for ID_x
15: **return**
16: **end if**
17: **do** with probability *p*
18: < *claim, signature* >← *signed_claim*
19: <ID_x, - , loc_x , $time_x$ > ← *claim*
20: *locations* ← pseudo rand(*rand*, ID_x, *g*)
21: **for all** *l* Є *locations* **do**
22: *a* → *l* : < ID_a , *l* , is_fwd_claim, *signed claim* >
23: **end for all**
24: **end do**
25: **else if** is_fwd_claim(*m*) then
26: < - , - , - , *signed claim* > ← *m*
27: < *claim, signature* > ← *signed_claim*
28: **if** bad_sig(*signed_claim*) or replayed(*claim*) **then**
29: discard *m*
30: **else**

```
31:                 < ID_x, - , loc_x , time_x  > ← claim
32:                 if detect_clone(memory, < ID_x, loc_x, time_x > ) then
33:                         trigger revocation procedure for ID_x
34:                 else
35:                         store fwd_claim in memory
36:                 end if
37:         end if
38:  end if
39: end Procedure
```

4.6 Secure & Robust RED.

The limitation in the RED algorithm is rectified in this algorithm. RED have limitations like, need for a centralized mechanism to transfer the *rand* value, unavailability of the seed infrastructure, communication cost for transferring the seed to all node. Instead of rand value this protocol takes current time as a seed for pseudo random function to select the witnesses. Hence this protocol [12] shows some improvement over RED. Also this protocol gives solution for the problem of mask replication attack by using watchdog mechanism.

V. Conclusion

In this paper we address one of the identity attacks in Wireless Sensor Networks called as Node replication attack. Different algorithms are developed for detecting this replication attack. These algorithms are classified in two schemes as Centralized and Distributed schemes. The Distributed detection scheme is preferred over the centralized detection scheme. Algorithms in both the schemes are having some lacunas which the recent algorithms tried to rectify. The recent research has more focus on the communication costs and energy efficiency of the algorithm. More focus is made on developing such algorithms. For future work the research can be made on these parameters.

References

[1] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala "Security in Wireless Sensor Networks: Issues and Challenges" Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia.

[2] Abhishek Jain, Kamal Kant, M. R. Tripathy "Security Solutions for Wireless Sensor Networks" Second International Conference on Advanced Computing & Communication Technologies 2012.

[3] R.Sathish, D.Rajesh Kumar "Proficient Algorithms for Replication Attack Detection in Wireless Sensor Networks – A Survey" IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013) 2013.

[4] Bryan Parno, Adrian Perrig, Virgil Gligor "Distributed Detection of Node Replication Attacks in Sensor Networks" 2006.

[5] Wibhada Naruephiphat, Yusheng Ji, Chalermpol Charnsripinyo "An Area-Based Approach for Node Replica Detection in Wireless Sensor Networks" 11th International Conference on Trust, Security and Privacy in Computing and Communications IEEE 2012.

[6] Choi H, Zhu S, La porta TF. "SET: detecting node clones in sensor networks". In: Proceedings of the 3rd international conference on security and privacy in communications networks and the workshops (SecureComm'07); 2007. p. 341–50, December.

[7] Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, Kandemir MT. "On the detection of clones in sensor networks using random key predistribution". IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 2007;37(November):1246–58.

[8] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei "Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN" 2006 IEEE International Conference on Systems, Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan

[9] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks" MobiHoc ACM ˝Montréal, Québec, Canada.

[10] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei "Distributed Detection of Clone attacks in Wireless sensor networks" IEEE transaction on dependable and secure computing September/October 2011.

[11] Zhao Jinchao "Research on Key Predistribution Scheme of Wireless Sensor Networks" Fifth International Conference on Intelligent Computation Technology and Automation 2012.

[12] Wazir Zada Khan, Mohammed Y Aalsalem, Mohamad Naufal Mohamad Saad "Secure & Robust RED" IEEE 2013.