EFFICIENT APPROACH TO DETECT NODE REPLICA IN WIRELESS SENSOR NETWORKS

[1]Mayur R. Khandekar, [2]Umesh K. Raut
[1]ME Student, MIT, Pune.[2]Assistant Professor, MIT, Pune.
Email:[1]mayurkhandekar11@yahoo.com

Abstract— Wireless sensor networks is emerging technology these days. There is very wide range of uses of this technology, from military purpose to medical purpose. The sensor are small and compact and can be deployed anywhere. These sensors are low in cost. So it performs important tasks for low cost. They can be deployed in hundreds to some thousands in quantity. This makes wireless sensor networks prone to different types of attacks. One of them is Node Replication attack. In this attack the attacker takes the Id of one legitimate node and make replica of it and place those node inside network. As sometimes the sensor transfers confidential data so it is important to protect it from these types of attacks. Different algorithms are developed to detect these replicated nodes. In this article we are proposing a detection algorithm that can be used to detect replication attack. This algorithm is named ND-RED(Neighbor Division-Randomize Efficient Distributed) Algorithm.

Index Terms— Algorithm, Replication Attack, Security Wireless Sensor Networks.

I. INTRODUCTION

These days Wireless Sensor Networks has wide range of applications. The Sensors are very low cost and are very compact in nature. So they can be deployed in large quantity. As Wireless sensor networks are often deployed in the areas where they cannot be monitored easily, and they are left unattended for long time. So, the attacker can physically capture one or more nodes from the network, extracts the important credentials(node id, keys) present on the node that are used for communication. Copy those credentials on one or more identical sensors and place those sensor nodes inside the network. As these nodes are having legitimate credentials these nodes acts as legitimate nodes inside the network and can communicate with other nodes present inside the network. This is called as Node Replication attack or Node Clone attack in Wireless sensor networks.

Different algorithms are developed to detect these node replicas and they are mainly categorized in two schemes, Centralized scheme and Distributed scheme, depending upon the nature of their defense. In Centralize detection scheme the replica detection is done at base station. In distributed detection schemes, detection algorithm runs on every node inside the network. These detection schemes use node id and geographical location of node to detect the replicated nodes.

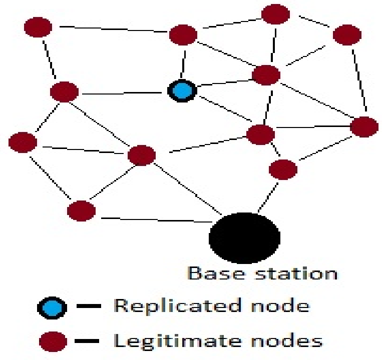

Fig 1 : WSN with replicated node

The rest of the paper is organized as follows : Section II gives the information about the related work. Section III gives the Assumptions. Section IV provides threat model. Section V gives proposed method. Section VI concludes the paper.

II. RELATED WORK

Different approaches were proposed to detect the replicated node in wireless sensor networks, these are mainly categorized in centralized detection schemes and distributed detection schemes. In centralized detection schemes the detection procedure is done at base station whereas in distributed detection schemes the detection algorithm runs on every node and any node can detect the replicated node.

In Straightforward method given in [4] each node transfers the list of ids of its neighbor nodes and geographical location to the base station, the base station then examines the list to look for nodes having same id but different geographical location, these nodes are consider as replicated nodes. This method is having very high communication cost. Communication cost is reduced in SET method given in [6] by Choi H et al. the set operations are performed on exclusive subsets of network, SET logically partition the network into non overlapping regions managed by leaders and these leaders respectively report to the base station, the intersection operation is performed on two subsets of reports. The result should be empty set otherwise replica is detected.

Another method proposed by Brooks R et al. in [7]. Detecting cloned keys algorithm is based on random pairwise key pre-distribution schemes. This is little bit different than the previous approach. It deals with the clones cryptographic keys rather than replicated sensor node ID's. In this algorithm the key usage is monitored if certain key is used more than the threshold value then that key is consider as cloned key.

Wibhada N. et al. proposed Area based approach to detect replicated nodes. Area based clustering detection combines the advantages of centralized approach and clustering approach. The network area is divided into three areas having 120 degree around the central node. Each node in particular area transfers its claim (node ID and location) to the witness node present in that area. The witness node checks for the conflicting claim. If not, then it transfers all claim to base station. The base station gets the claim from all areas, then the base stations checks for conflicting claim.

Following are the drawbacks for centralized Detection schemes.

1. Base station becomes the Single point of failure.
2. The nodes around the base station exhaust very rapidly compared to other nodes in the network due to heavy traffic towards base station through these nodes.
3. The base station cannot start the detection till it will not get all the claims so making the procedure slow.
4. Some sensor networks do not have powerful base station to execute algorithms properly.

Distributed detection schemes are developed, to deal with the demerits of centralized detection schemes. In Node to network broadcast method proposed by Bryan P. et al. in [5] each node broadcast its location information to whole network, each node stores the location information of its neighbor and if it receives the claim conflicting with the claim of its neighbor, replica is detected.

All of next algorithms follow Claimer-Reporter-Witness pattern. A claimer node generates claim (node ID and geographical location) and transfers this claim to reporter nodes. Reporter nodes transfer this claim to Witness nodes. Detection is performed at the witness nodes If the witness come to know that it received two claims having same node id but are present at different geographical locations, it consider them as clone nodes.

In Deterministic multicast given in [4] the witness nodes are chosen as a function of node's ID. If the attacker replicates a node (Copies node id of other node) then for both the replicas, same witness node will be chosen. The witness will receive two different claims for same node ID. As witness selection is deterministic the attacker can compromise the witness node beforehand. So another algorithm called Randomize Multicast was proposed is proposed by Bryan P. et al. that randomize the witnesses for a given node's location claim, so that the adversary cannot anticipate their identities. Line selected multicast proposed in [4] reduces the communication overhead and improves the detection probability compared to Randomize multicast. For a location claim to travel from reported node to witness nodes, it must pass through several intermediate nodes as well. If these intermediate nodes also store the location claim, then a line can be effectively drawn across the network. If a conflicting location claim ever crosses the line, then the node at the intersection will detect the conflict and initiate a revocation broadcast. In Randomize Efficient Distributed algorithm (RED) proposed by Conti et al. in [9] the witness nodes are chosen Pseudo randomly. A Pseudorandom function takes Claimer node ID and Rand value broadcasted by base station as arguments and generates the ID's of witness nodes. Red algorithm requires centralize system to transfer the rand value to whole network. This is some added overhead. This overhead is removed in Secure & Robust RED (SR-RED) proposed by Wazir Z. et al. in [11] that takes current time as the rand value for the pseudorandom function.

III. Assumptions

We consider a sensor network with low cost nodes. The nodes are distributed over a wide area and they can communicate with each. Each node in the network has unique ID. Every node can communicate with each other. The ID's are assigned to nodes at the time of deployment. The adversary cannot create new ID's for any replicated nodes. At least one reporter node should not be compromised node. Replicated node will follow the detection algorithm in normal way so that it will not found as outlier.

IV. Threat Model

- As most of the network contains nodes that are not tamper proof, adversary can capture a sensor node, extract security credentials on the node. Create replica of that node by inserting the same credentials that are extracted from the captured node.
- The compromised nodes and replicas are controlled
  by the adversary and can communicate with each other.
- Adversary tries to prevent clones from being detected by detection algorithm.

V. Proposed Method

A. Parameters.

1. Detection Probability: Probability that the detection technique will find the replicated node.
2. Communication cost: Total number of messages sent by all the nodes together.
3. Memory overhead: Total number of messages stored in memory of nodes.
4. Energy consumption: Energy of node consumed by the algorithm in single iteration.

B. Neighbor Division- Randomize Efficient Distributed (ND-RED) Algorithm.

Our propose is to find the replicated node inside the network with less energy consumption, minimum number of message stored, min communication cost and high detection probability. While working on the RED algorithm we find some gap where we can work. In RED algorithm, the neighbor nodes transfer the claim to the witness nodes with some probability P. In a randomly deployed network the present RED algorithm will show low detection probability for the claimer nodes having less neighbor nodes and less P value. Suppose that the nodes are having 30 neighbors. Then with p=0.1 the detection probability of RED is 0.95(i.e.$(1-(1-0.1)^{30})^2$). But for nodes having 5 neighbors the detection probability is 0.162 (i.e.$(1-(1-0.1)^5)^2$). The detection probability can be increased by increasing the value of P from 0.1 to 0.5. But if we increase the value of P the communication cost, storage overhead, Energy consumption by the algorithm increases as large number reporter nodes will transfers claim to the witness node. So we proposed a detection method that will show good detection probability for the nodes having less neighbor nodes with controlling the overheads.

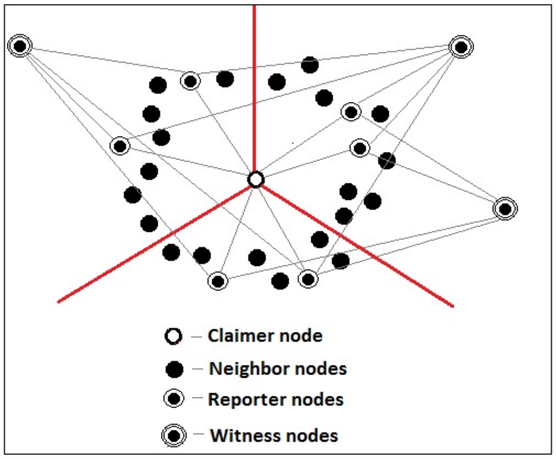

Fig 2. ND-RED

In RED algorithm the claimer node broadcasts signed claim to all its neighbor nodes and these neighbor nodes acting as reporter nodes transfer the claim of claimer node to the pseudo randomly generated witness nodes with some probability P. Adi Shamir proposed a signature scheme in [12]. Due to above reasons RED creates communication and storage overhead, also the energy consumption is more if neighbor nodes are high and P value is high. So we are working on these parameters. We divide the neighbor into different areas and randomly selects x neighbors from each area. This are now called as the reporter nodes. And only these reporter nodes will transfer the signed claim of the claimer node to the witnesses with some probability P.

This change decreases the no of message transfer, also only some limited nodes need to store the claim reducing the memory occupancy. Transferring and receiving the location claim, signing, verifying signatures consumes some energy of the node, as less no of claims are transferred energy consumption will be less as compared to original RED algorithm. At the end we will compute the values of these parameters for the existing algorithm and our proposed algorithm. We are comparing the values of parameters for both algorithms.

C. Simulation Results:

As we are in the initial phase of implementation, we have initially calculated the energy consumption of the nodes for single iteration of both the algorithm and compared the results for both the algorithms. We are using JUNG framework for simulation.

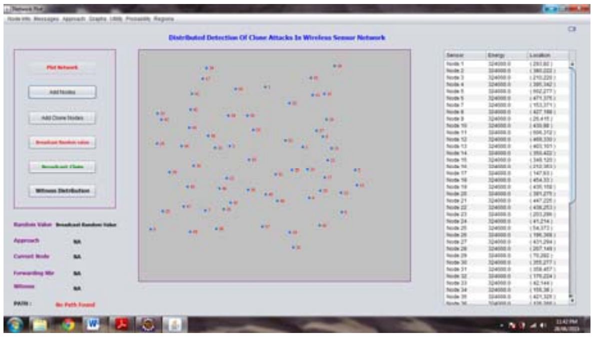

Fig 3. Simulation

In simulation we are working on 60 nodes. We executed both the algorithms are calculated the value of energy consumption for both algorithms. Fig 4 shows the energy consumption comparison analysis for RED and ND-RED on 60 nodes with p=0.5

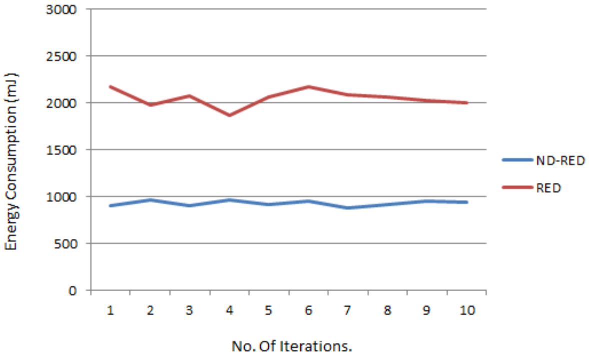

Fig 4. Energy Consumption analysis for 60 nodes.

From the simulation results we can see that the energy consumption in less in our system.

VI. Conclusion

In this paper, a unique problem in WSN security known as the node replication attack is addressed. We reviewed various detection algorithms. RED is assumed to be the best algorithm, considering its simulation results. We are making an attempt to improve this algorithm, and we come up with a new algorithm called Neighbor Division-RED (ND-RED). This algorithm is modified version of existing RED algorithm. The simulation result shows that the energy consumption of our algorithm is less as compared to the RED.

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), Melaka, Malaysia, pp. 357-59, 1-3 July 2013.

[2] Abhishek Jain, Kamal Kant , M. R. Tripathy "Security Solutions for Wireless Sensor Networks" Second International Conference on Advanced Computing & Communication Technologies pp. 430-33, 2012.

[3] R.Sathish, D.Rajesh Kumar "Proficient Algorithms for Replication Attack Detection in Wireless Sensor Networks – A Survey" 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN) pp.1-6, 2013.

[4] Bryan Parno, Adrian Perrig, Virgil Gligor "Distributed Detection of Node Replication Attacks in Sensor Networks" pp.1-9, 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 pp.745-49, 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). pp.341–50, December. 2007.

[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 pp.1246–58, November 2007.

[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, Taipei, Taiwan. pp.1468-72 October 8-11, 2006

[9] 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 pp. 685-94 September/October 2011.

[10] Zhao Jinchao "Research on Key Predistribution Scheme of Wireless Sensor Networks" Fifth International Conference on Intelligent Computation Technology and Automation pp. 287-90, 2012.

[11] Wazir Zada Khan, Mohammed Y Aalsalem, Mohamad Naufal Mohamad Saad "Secure & Robust RED" IEEE pp. 1-5, 2013.

[12] Adi Shamir "Identity-Based Cryptosystems and Signature Schemes" Advances in Cryptosystems - CRYPTO '84 pp 47-53, 1985.