Zone Based Node Replica Detection in Wireless Sensor Network Using Trust

Soumya Sara Koshy [#1], Sajitha M [*2]

[#1] *MTech student (CSE), MES College of Engineering, Kuttippuram, India*

[#2] *Assistant Professor (CSE), MES College of Engineering, Kuttippuram, India*

Abstract— A wireless sensor network is a group of sensor nodes. Sensor senses the environment, process data and communicates wirelessly over a short distance. Wireless sensor network has been used in various critical applications. Hence security is of prime concern. The node replication attack is one in which an adversary captures a sensor node and creates copies of the captured sensor node. These newly created copies called clone nodes will be placed at strategic locations in the network, from where they can provide many insider attacks. Replica node will act like an authenticated sensor node. Hence it will be very difficult to detect the clone nodes. In zone based node replica detection with trust, the entire network is divided into a number of zones and node replica detection is done based on the values of trust values calculated.

Keywords— Node replication, Wireless Sensor Network, Witness nodes, Zone leader.

I. INTRODUCTION

A wireless sensor network is a new technology for gathering critical information. Wireless sensor networks consist of a number of sensor nodes. Sensor nodes gather information within their sensing area and sends to a central base station.

Wireless sensor networks are generally unattended. Hence susceptible to various attacks. The attack may target not only the physical integrity of nodes but also the data transmitted within the network. Also due to the critical applications of wireless sensor network, security is of prime concern.

Sensor nodes are not provided with any tamper resistant hardware. So it becomes easier for an adversary to capture and compromise a sensor node. In node replication attack an adversary captures a sensor node, extracts the information about the node and produces copies of the captured node. All the newly formed nodes called clone nodes will be having the same ID as that of the captured node. Clone nodes are treated as legitimate nodes and hence it will be very difficult to detect them. Once the clone nodes gain the trust of other sensor nodes, they will perform many malicious activities. Hence it is very important to detect the clone nodes.

II. RELATED WORKS

In Centralized scheme [1] each node sends a list of its neighbours and their claimed locations to the base station. The base station then examines the neighbour list to detect the replica nodes. If replica nodes are found, the base station will revoke the replicated node by flooding the network with an authenticated revocation message.

In distributed approach [1] location information of each node is stored at one or more witness nodes. The location information of newly joined nodes is forwarded to the corresponding witness nodes. Witness nodes on the reception of two location claims from the same ID can detect the presence of replica node. Node-To –Network broadcasting and Deterministic multicast are two distributed approaches. In Node-To-Network Broadcasting each node stores the location information for its neighbours and if it receives a conflicting claim, revokes the offending node. If an adversary can jam key areas or interfere with communication paths, this method cannot achieve 100% detection. Also the total communication cost for each node is high. In Deterministic multicast a nodes location claim is shared with a limited subset of deterministically chosen witness nodes. But this method has high communication cost. Since deterministic, the adversary can also determine the witness nodes. It cannot afford a large number of witness nodes.

Parno et al. proposed two new distributed approaches namely Randomized multicast and Line selected multicast.

In Randomized multicast [1] each of the node's neighbours probabilistically forwards the location claim to a randomly selected set of witness nodes. If any witness node receives two different location claims for the same node ID, it can revoke the replicated node. The birthday paradox ensures that two conflicting claims have a high probability of sharing a common witness node. In line selected multicast [1] all intermediate nodes from a node to a destination node will also store location claims as a line. A node on the line-crossing point will detect a conflict, if conflicting location claim line crosses the node. Line-Selected Multicast has a lower communication cost compared to Randomized Multicast.

Conti et al.[2] proposed a randomized efficient and distributed(RED) protocol for the detection of node replication attacks. In RED initially a random value, is shared among all nodes. After that d each node broadcasts its id and location claim. For each node, each of its d neighbours sends the claim to a set of pseudo randomly selected network locations. RED executes at fixed intervals of time. Pseudorandom function guarantees that the witnesses for a location claim are unambiguously determined for a given protocol iteration.

In localized multicast proposed by Zhu et al. [3], the witness is randomly selected from a geographically limited region of nodes, called a cell. This approach deterministically maps a nodes ID to one or more cells. Randomization is used within the cell(s) to increase the resilience and security of the scheme. Two variants of the Localized Multicast approach have been proposed: Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In SDC [3], using a geographical hash function each node is mapped to a single destination cell. Each node in the destination cell independently decides whether to store the claim. On reception of different location claims with the same ID, destination cell can detect the presence of replicating. In the P-MPC [3] scheme, the location claim is mapped and forwarded to multiple deterministic Cells with various probabilities.

Choi et al [4] proposed SET [4] in which one hop neighbours are grouped into non overlapping sub regions. There is a central base station and the report of each subset is transmitted to the base station. Node ID’s are unique and hence the intersection of the sub region must be empty. A tree structure is formed over the sub regions for computation of set intersection.

In Distributed detection with group deployment knowledge proposed by Ho et al.[5], a group deployment strategy is used. Sensor nodes are grouped together and programmed with the corresponding group information before deployment. Sensor nodes are deployed in groups. Each group of nodes is deployed towards the same location called the group deployment point. The group members will exhibit similar geographic relations.

Zeng et al.[6] proposed a Random Walk Based Approach [6] in which witness selection is distributed to every passed node of random walks. The adversary cannot easily find out the critical witness nodes. Two methods: Random Walk (RAWL) and Table Assisted Random Walk (TRAWL). In Random Walk [6] neighbours of a node probabilistically forwards the location claim of the node in some randomly selected nodes in at step random walk. Each randomly selected node sends a message containing the claim to start a random walk in the network, and the passed nodes are selected as witness nodes and will store the claim. Table Assisted Random walk [6] is employed to reduce the memory costs of RAWL protocol. Traces of random walk are recorded at each node using a trace table. Each passed node does not want to store the location claims.

Mishra et al.[9] proposed a zone based node replica detection scheme. In ZBNRD entire network is divided into a number of zones. Each zone has a zone leader and the zone leaders will share their membership list among themselves. Replica detection is done by zone leaders.

III. PROBLEM DEFINITION

The node replication attack is a serious threat in wireless sensor networks. Such attacks need to be detected as early as possible. Various methods have been discussed to detect the node replication attacks. Even though we can successfully detect node replication attacks using these methods there are several drawbacks for each of them in terms of memory efficiency, energy efficiency, communication efficiency and detection probability. Earlier centralized approach suffers from a single point of failure. Distributed methods discussed are nondeterministic, so it is easier for an adversary to detect the witness nodes. Also they suffer from memory and communication overhead. Also they are location dependent. Some of the methods have low detection probabilities. The method zone based node replica detection scheme is efficient to a certain extent in which it is not location dependent. Detection probabilities are also comparatively better. But still it suffers from communication and message overhead. Also it is based on key management. The method can be improved further based on trust.

IV. PROPOSED WORK

In the proposed work, zone based node replica detection with trust; the network is divided into a number of zones. Zone leaders are selected prior to deployment and zone is formed dynamically. Zone leaders will detect the replica nodes based on a trust factor. Trust values will be calculated for each node and replica nodes are detected based on these calculated trust values. The node information is checked. Trust values are checked and updated for each node. Node replica detection is done on the basis of trust values. Prior to zone formation trust values are checked and updated. Thus the replica nodes can be detected. Flow chart of the proposed method is shown in figure I.

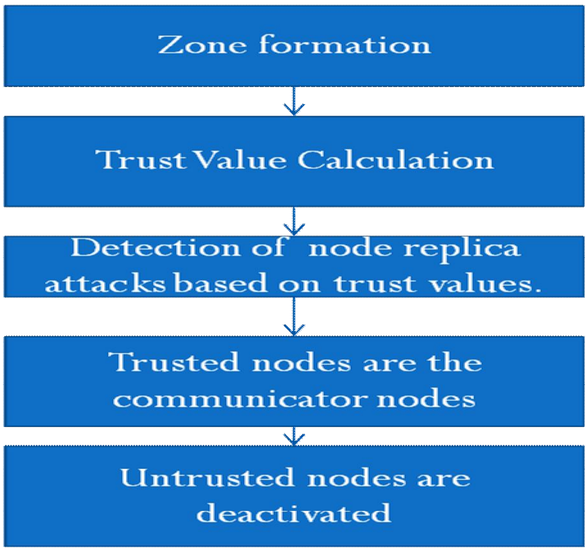
Zone formation
Trust Value Calculation
Detection of node replica attacks based on trust values.
Trusted nodes are the communicator nodes
Untrusted nodes are deactivated

Figure I: Proposed method

V. IMPLEMENTATION DETAILS

The project is simulated using the NS-2 simulator. Nodes are static, non-tamper resistant, and are uniformly deployed in the area of observation. Communication links are bidirectional. There is no centralized trusted entity. At the beginning of the simulation various parameters of the sensor nodes have been defined. Nodes are assigned with a unique ID, prior to their deployment. The work includes the following modules.

- Zone Formation.
- Trust Management.
- Replica Detection
- Performance analysis

A. Zone Formation

The network is divided into a number of zones. Each zone will be having a predetermined zone leader. Zone leader will be sending messages to one hop neighbours, which in turn will be sending to their one hop neighbours and so on. Nodes respond to the zone leaders by sending a message back in order to join a particular zone. The route discovery process involves sending route-request packets from a source to its neighbour nodes, which then forward the request to their neighbours, and so on. Once the route-request reaches the destination node, it responds by unicasting a route-reply packet back to the source node via the neighbour from which it first received the route-request. When the route-request reaches an intermediate node that has a sufficiently up-to-date route, it stops forwarding and sends a route-reply message back to the source.

B. Trust Management

Trust is calculated based on four parameters. Energy, bandwidth, node joining and node leaving are the parameters used. Trust values are calculated for each node. Trust values are calculated for each node.

C. Replica Detection

Replica detection is done by the zone leaders. Zone leader will check the trust values of each node. If a node will be having a lower energy than the threshold set, then a negative point will be given. Also the bandwidth of each node is compared with a threshold. If a node joins a network by sending a proper join request, then a positive value is assigned. If abnormal joining then a negative point is assigned. Based on the calculated trusted values a node will be given a certificate authority if it is trusted. If any node fails to get a certificate authority, then that node is a replica node.

D. Performance Analysis

The network is divided into zones. The trust factor is added. Trust information of each node is checked and updated. Average trust values calculated for each node is shown in figure II. If a node has lower trust value then it is a replica node.

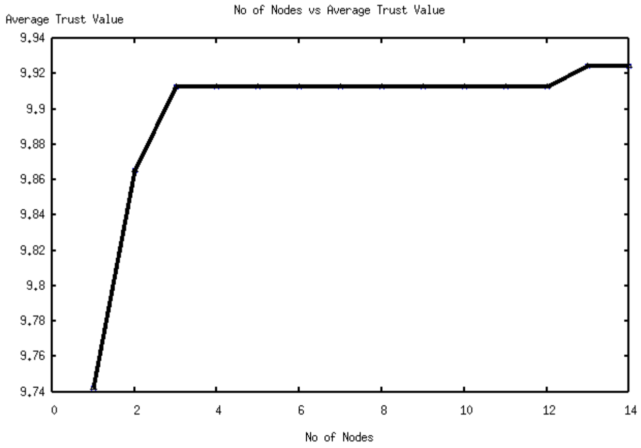

Figure II: Average Trust values of nodes

The packet delivery ratio has been improved. Figure III shows the packet delivery ratio of the proposed method plotted against zone based node replica detection.

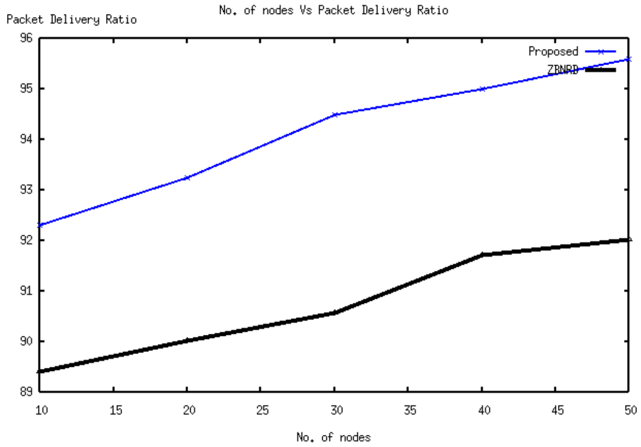

Figure.III Packet delivery ratio of zone based node replica detection with trust plotted against ZBNRD.

End to end delay have been improved .In figure IV. End to end delay of the proposed method is plotted against ZBNRD.

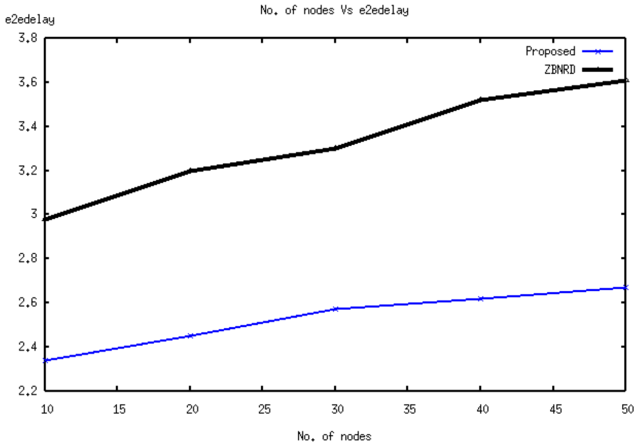

Figure IV: End to end delay of proposed method plotted against ZBNRD.

VI. CONCLUSIONS

The Wireless Sensor Network is an emerging area which has wide applications. Hence the security in wireless sensor network is of great concern. Node replication attacks are an important attack against a wireless sensor network in which an adversary compromises a sensor node and creates copies of that node and deploying it in strategic areas. Various methods have been developed in order to detect the node replication attacks. Zone based node replica detection using trust is an enhanced method using trust which improved the packet delivery ratio and reduces the end to end delay.

REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In Security and Privacy, 2005 IEEE Symposium on, pages 49 - 63, may 2005.

[2] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. A randomized, effcient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '07, pages 80-89, New York, NY, USA, 2007. ACM.

[3] Bo Zhu, S. Setia, S. Jajodia, S. Roy, and Lingyu Wang. Localized multicast: Efficient and distributed replica detection in large-scale sensor networks. Mobile Computing, IEEE Transactions on, 9(7):913-926, july 2010.

[4] Heesook Choi, Sencun Zhu, and Thomas F. La Porta. Set: Detecting node clones in sensor networks. In Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on, pages 341 -350, sept. 2007.

[5] Jun-Won Ho, Donggang Liu, Matthew Wright, and Sajal K. Das. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. Ad Hoc Netw., 7(8):1476-1488, November 2009.

[6] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie. Random-walk based approach to detect clone attacks in wireless sensor networks. Selected Areas in Communications, IEEE Journal on, 28(5):677 -691, june 2010.

[7] Lee-Chun Ko, Hung-Yuan Chen, and Guan-Rong Lin. A neighbor-based detection scheme for wireless sensor networks against node replication attacks. In Ultra Modern Telecommunications Workshops, 2009. ICUMT '09. International Conference on, pages 1 -6, oct. 2009.

[8] Ming Zhang, V. Khanapure, Shigang Chen, and Xuelian Xiao. Memory efficient protocols for detecting node replication attacks in wireless sensor networks. In Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on, pages 284 -293, oct. 2009.

[9] AlekhaKumar Mishra and AshokKumar Turuk. A zone-based node replica detection scheme for wireless sensor networks. Wireless Personal Communications, pages 1-21, 2012.