Detection of Node Replication Attacks in MSN Using EDD Algorithms

Pooja Mishra[1], Gaurav Gupta[2]

[1] Lecturer, Dept. Of Computer Engineering, Pad Dr D Y Patil PolyPune,MS,India.
[2] Lecturer, Dept. Of Computer Engineering, Pad Dr D Y Patil PolyPune,MS,India.

---***---

Abstract - Node replication detection is a challenging problem. Though the defending against node replication attacks demands immediate attention as compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented. Additionally, whereas most of the presented schemes in static networks exist on the witness-finding strategy that cannot be applied to mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks incurs efficiency and security problems. Thus, based on our devised challenge-and-response and encounter-number approaches, required algorithms are proposed to resist node replication attacks in mobile sensor networks. The advantages of our proposed algorithms include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance**.**

Key Words**: Attack, security, wireless sensor networks, Cluster, XED, EDD.**

1.INTRODUCTION

Wireless Sensor Networks (WSNs) have been used in various applications, e.g., military, environmental, and health applications [1]. When WSNs are deployed in hostile scenarios, such as surveillance on the battlefield, they must confront the threats from attackers (e.g., enemies on the battlefield). This is because the attackers may intend to learn Wireless sensor networks are susceptible to node replication attacks due to their unattended nature. Existing replicas detection schemes can be further improved in regard of detection probabilities, detection overheads, and the balance of detection overheads among sensor nodes. In this paper, we make the following contributions: first, we point out the unrealistic assumption that the replica node would behave honestly as the benign sensor nodes; thus the existing detection schemes would fail if the replica nodes cheat or collude with the compromised node.

Replication attack is one of the insider threats. The attacker captures one or more sensor nodes, tampers with them and obtains the credential materials, such as the identity and keys, then clones some nodes as replica nodes, and surreptitiously inserts these replicas in the network. Subsequently, the attacker may launch a variety of insidious attacks, such as data injection, selecting forwarding, routing loop, or even topology partition. Just as shown in Figure 1, a network was formed by the normal nodes (without frame). The captured and compromised nodes are represented in the solid frame, and replica nodes are represented in the dashed frame. Thus, detection of replica nodes becomes one research hotspot in WSN. The first distributed replication detection schemes RM and LSM were proposed by [2]. In RM scheme, nodes broadcast to neighboring nodes the location claim message signed by ID-based public key scheme. Then the neighbors forward such received claim message with a specified probability to randomly selected network nodes, which act as witness.

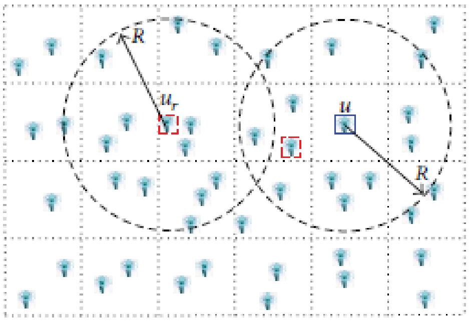

Fig -1: Replication Attack in Wireless Sensor Attack.

2. RELATED WORK

2.1Static Methods

1. Techniques Related With Witness Finding:

In this Techniques central node ask every node to prove his identity. Node used neighbor node as there witness to prove their identity. This method has drawback that it detect only static network & not mobile network plus this method is very slow as detection is done centrally.

2.Techniques Related with predistributed Keys.

In this method pre distributed keys are used that will used public key cryptography to detect fake node. This method works only for static network.

3.Techniques Related with Random Clustering.

In this method nodes are group together in various cluster. This helps in finding out fake node which are not part of cluster this method work only for static network.

2.2Mobile Methods

1. Techniques Related with distributed detection.
   In this method no central node is used for detection. Detection is done by neighboring node using distributed approach. This method work for mobile networks but its storage requirement is high.
2. Techniques Related with centralised detection.
   In this method a central node decides a velocity for all nodes in the network all nodes move with same velocity. As fake node does not move with velocity of the network it easily gets detected. This method work for mobile network but it is manage from central node.
3. Techniques Related with local information Exchange.
   In this method various local nodes exchange the information which is used for fake node detection there is requirement for time synchronization.
4. Techniques Related with mobility.
   In this method distributed algorithm is used & every node keeps list of all location .it has visited in the past. Each mode then broadcast this information to all other node this way fake node can be detected. This method generates extra overhead by broadcasting.

2.3 Detection Techniques for Mobile WSN.

The node replica detection techniques developed for static WSNs. It do not work when the nodes are expected to move as in mobile WSNs. As a result some techniques have also been proposed for mobile WSNs. These techniques are improved to detect the replica node. These techniques are characterized into two main classes as centralized and distributed techniques.

2.3.1 Centralized Techniques:

1. Sequential Probability Ratio Test (SPRT): SPRT ,which performs the following steps: In mobile sensor network each and every time a mobile node moves one location to another location , each of its neighbors asks for a signed claim containing its location and time interval information .It decides probabilistically whether to forward the received claim to the sink node. The sink node computes the speed from every two successive claims of a mobile node and performs the SPRT by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node; it will promote the random cross the upper limit and thus edge to the sink node accepting the alternate hypothesis that the mobile node has been replicated. On the other hand, each time the maximum speed of the mobile node is not reached; it will promote the random cross the lower limit. The sink node accepting the null hypothesis that mobile node has not been replicated and alternate hypothesis has been replicated. The exchange Hypothesis is accepted, the replica nodes will be removed from the network.

2.3.2. Distributed Techniques

1. Extremely Efficient Detection (XED): extremely Efficient Detection (XED), it's against the node replication attack in mobile sensor network. The idea behind XED is motivated from the observation that for the networks without clones, if sensor node i meets another sensor node j at earlier time and I sends the random numbers to j , i and j meets again and again , i can assertion weather this is the node j met before requesting the random number r. This techniques developed to, challenge-and-response and encounter-number, are fundamentally different from the others. The two sensor nodes i and j within the communication ranges of each other, first it will generate the random numbers and it will exchange their generated random numbers. The generated random numbers and received random number in their respective memory. To generate the random number they use the cryptographic hash function to store the node value. Here the replica does not possess the correct random number. This node can be attributed to the fact that each node detects the replica by itself and will detect the replica at different time period. The XED scheme is composed of two steps: online step and offline step. In offline step security parameter cryptographic hash functions stored in each node.

2. Efficient and Distributed Detection of Node: The idea behind EDD is motivated by some observations. For a network without replicas, the number of times, X1, in a node U encounters a particular node V, should be limited with the time period with high probability. The replicas V, the minimum number of times, X2, in which U encounters the replicas with same ID V, should be larger than a threshold within the equal time period. According to these observations, if each node can discriminate between these two cases, every node has the ability to identify the replicas. The EDD scheme is composed as two steps: offline step and online step .The offline step performed by the network before the sensor deployment. The objective is to calculate the parameters, length T of the time interval and threshold used for discrimination between the honest nodes and the replica nodes. The online step performed by each node per move. Each node checks the encountered nodes are replicas with the corresponding number of encounter at the time interval period. It has the lower communication overhead.

3. NETWORK MODEL AND ASSUMPTIONS

We assume that there are only stationary sensor nodes in the wireless sensor network .We also assume that the communications between the stationary sensor nodes are bidirectional ,which is also an assumption of most of previous detection schemes .Stationary nodes can get their geographic location by using positioning device (e.g., GPS device) or positioning algorithms [3-5]. Also, we assume that all the sensor nodes are loosely time synchronized using time synchronization Techniques.

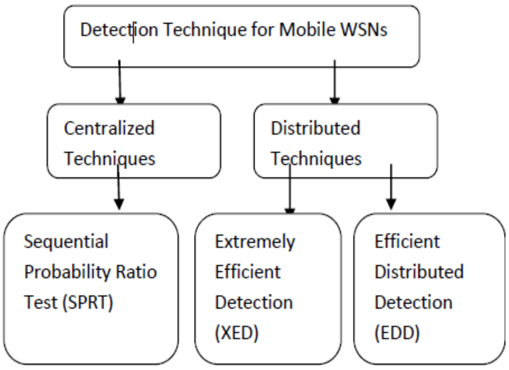
Detection Technique for Mobile WSNs
Centralized Techniques
Distributed Techniques
Sequential Probability Ratio Test (SPRT)
Extremely Efficient Detection (XED)
Efficient Distributed Detection (EDD)

Fig -2: Detection Technique for MSN.

3.1 Security Model:

In our methods, sensor nodes are not tamper-resistant. In other Words, the corresponding security credentials can be accessed after sensor nodes are physically compromised. Sensor nodes could be compromised by the adversary immediately after sensor deployment. The adversary has all of the legitimate credentials from the compromised nodes. After that, the adversary deploys two or more nodes with the same ID; i.e., replicas, into the network. Replicas can communicate and collude with each other in order to avoid replica detection in EDD For example; replicas can share their credentials and can selectively be silent for a certain time if required after the collusion. Owing to the use of the digital signature function [10], [11], the replicas cannot create a new ID or disguise themselves as the nodes being not compromised before, because it is too difficult for the adversary to have the corresponding security credentials. Since the focus of this paper is on the node replication attack, despite many security issues on sensor networks such as key management, replay attack , wormhole attack , Sybil attack , secure query, etc., can be handled in our proposed work.

4. PROPOSED METHOD

4.1 L-EDD Algorithm:

The LEDD algorithm is an enhancement of EDD algorithm to support differentiation of delay and losses. It uses similar mechanism as in Round Robin algorithm to choose next packet/cell to service. We expect that such modified EDD scheduler will better treat good behaving flows in present of overload (e.g. caused by misbehaving sources).

To decrease complexity of algorithm we did not apply the sorted queue. LEDD algorithm uses multiple FIFO system to serve flows with different deadlines TD. Using of such a system allows aggregation of flows into classes according to their deadlines. We assume that the range of deadline values is limited. Deadlines assigned to cells are not continuous set of values, but belong to defined, finite subset D={d1; d2; ...; dn), where n is the number of classes. Next, such classified traffic is served by multiple FIFO system, where a single FIFO queue is assigned for each of class. The main assumption for LEDD is that for each class (FIFO buffer) a limit counter LC is assigned.

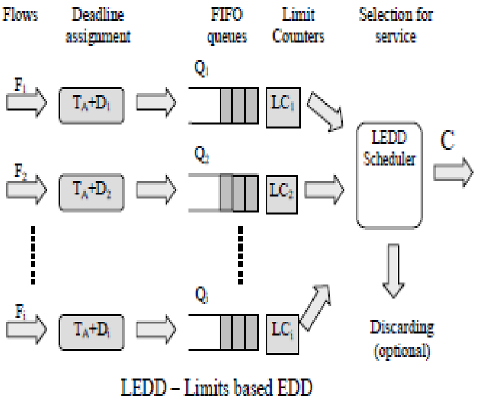

Fig -3: The proposed LEDD algorithm – deadline and limit based EDD scheduling.

The selection to service of particular packet/cell is based on the following rule:

1. A cell with smallest deadline time TD from buffers is chosen for service, but only if limit LC of buffer storing the cell is greater than zero;
2. If the cell was selected to service from a buffer, then limit LC assigned to this buffer is decreased by 1;
3. The buffer which limit is exhausted does not participate in process of searching cell for service, with exception described in the next point;
4. if the buffer/buffers with positive limit are empty, then searching cell in another buffer (with limit equal to zero) is allowed;
5. If all buffers' limits reach zero, then limits are set to their initial values.

When the limit of a particular flow reaches zero, then appropriate buffer is temporary unavailable for the server. Traffic waiting in such a buffer suffers large delay and losses due to its increased deadline violations ratio. But it is profit for other classes, especially to those with larger limit. Limit Counter assigned to each buffer counts successful entering of a Counter.

There were three tests provided to investigate behavior of proposed algorithm. The first and second test compared abilities of Classic EDD and L-EDD algorithms for providing delay and losses differentiation respectively. The second test examined handling of CBR traffic in the presence of congestion caused by traffic with Poisson characteristics.

Incoming traffic was Poisson distributed in the first two tests. The third test was performed using CBR sources with Poisson traffic in the background. Results of simulation were obtained during simulated time interval, which provided at least several millions of events.

4.2 Reactive at low traffic load and proactive when the traffic load is high.

Energy Aware Geo-location aided Routing (EAGER), this protocol partitions the network into disjoint and equal-sized cells and performs intra-cell proactive routing and inter-cell reactive routing. The design of the intra-cell and inter-cell routing schemes fully utilizes the cell structure of EAGER Thus, EAGER belongs to the topology-based approach and differs from the position-based routing protocols. To our best knowledge, EAGER is the geo-location aided routing protocol that utilizes only the self-location information.

EAGER relies on self-location information to partition the network into disjoint proactive cells. The structure of disjoint cells significantly reduces the percentage of nodes involved in a route discovery process. then optimal cell size and transmission range are obtained analytically in Eager while simulations are resorted to in ZRP to obtain the zone radius. The performance measure used in EAGER also differs from that of ZRP, the former being energy efficiency and the latter routing overhead.

4.3 Route Discovery

For networking, route needs to be established before message transmission. We consider a hop-by-hop routing protocol As illustrated in Figure 3,when source A has a message for Z, it initiates a route discovery process by broadcasting a request using the network paging sequence to wake up all its neighbors. The request packet contains the source address, the destination address, and a hop count which is zero initially.

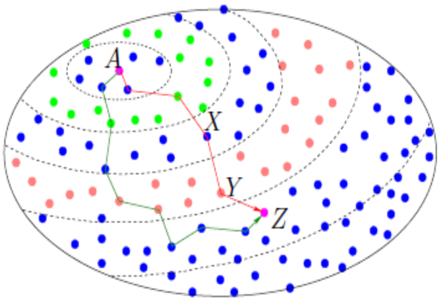

Fig 5: Route Discovery.

A neighboring node decodes the request packet, replaces the source address with its own, sets a reverse pointer to the transmitting node, increases the hop count by one, and broadcasts the new request packet. In Figure 3, two different routes from A to Z are illustrated.

5. EVALUATION and SIMULATION RESULTS.

5.1 Metrics

We used the following metrics to compare the schemes:

- Communication Overhead: We measured the total number of packets sent and received for running the replica detection algorithm when n nodes are added to the network. We denote this metric as nf .
- Success rate in detecting replicas We measured the probability of detecting a replica, when there are two sensors with the same identity in the network, i.e. p2r.

6. CONCLUSION AND FUTURE WORK.

In this paper, apart from two replica detection algorithms for mobile sensor networks, XED and EDD, we proposed the L-EDD algorithm. The algorithm has properties which make it suitable for handling streaming traffic in a mobile sensor network. The simulation results for two serviced classes which show that L-EDD algorithm allows differentiation of loss ratio among classes. The differentiation is relative which means that improvement of performance for one class implies degradation of another one. Simulation tests were performed for two types of traffic, Poisson and CBR. Additionally, simulation results proved that there is a possibility to create a privileged class, with stringent requirements concerning delay and losses. Especially, CBR traffic can be handled with practically no losses.

Additional advantage of L-EDD is that it has simpler implementation than Classic EDD. By using multiple FIFO system maintaining of sorted queue is no longer needed.

Future work should include finding the method of limits assignment for handling different types of traffic.

REFERENCES

[1] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T.Kandemir,"On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern. C, Ap- plicat. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[2] M.Conti, R.D.Pietro, L.V.Mancini, andA.Mei, "Arandomized, efficient and distributed protocol for the detection of node replication at- tacks in wireless sensor networks," in Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Montreal, Canada, 2007, pp. 80–89.

[3] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. De- pend. Secure Comput., vol.8,no. 5, pp. 685–698, Sep./Oct. 2012.

[4] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor

BIOGRAPHIES

Mrs.Pooja Mishra was born in Nagpur , India, in 1983. I received the B.E. degree in computer Engineering from the University of Rastrasant Tukdoji Maharaj University, Nagpur, India, in 2007, and the M.E degree in Computer Engineering from Savitribai Phule University,Pune, India, in 2015 respectively.

Since August 2011, I have been with the Department of Computer Engineering ,Pad Dr D Y Patil Poly ,where I am working as a lecturer and my current research interests in Wireless Networking.

Mr.Gaurav Gupta was born in Jalna , India, in 1990. I received the B.E. degree in computer Engineering from the University of North Maharashtra University, Jalgaon, India, in 2011, and the M.Tech degree in Computer Science and engineering from Jawaharlal Nehru Technical University Hyderabad, India, in 2016 respectively.

In 2011, I have joined BEL Bangalore, as a DBA, and in 2013 I have switched myself toward lectureship. Since September 2013, I have been with the Department of Computer Engineering ,Pad Dr D Y Patil Poly ,where I am working as a lecturer and my current research interests include data mining and Networking.