AN APPROACH TO DETECT NODE REPLICATION IN MOBILE SENSOR NETWORKS- SURVEY

P. Edith Linda¹, R. Sangeetha²

Assistant Professor, Department of Computer Science, G.R.Damodaran College of Science, Coimbatore, Tamilnadu¹

M.Phil Scholar, Department of computer Science, G.R.Damodaran College of Science, Coimbatore, Tamilnadu²

ABSTRACT:

In mobile sensor network (MSN), there are many nodes and they are unattended so an adversary can easily attack and compromise the sensor nodes and take private key from the nodes. In this paper we mainly focus on the detection of replication node in mobile sensor networks. Several algorithms are developed to detect the replica attacks, in static WSNs and mobile WSNs. Every technique has its own advantages and disadvantages. In recent years, detection of replication node is an important task to detect the node in wireless sensor network area. In our survey, we analyze previous year research and contributions of the existing techniques are Random key Pre distribution, SET, Deterministic Multicast, Randomized Multicast and Line Selected Multicast, Randomized Efficient and Distributed Mechanism, Localized Multicast, Sequential Probability Ratio Test, eXtremely Efficient Detection, Efficient And Distributed Detection.

Keywords: mobile sensor network, clone attack, witness Node

INTRODUCTION:

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that co function in order to achieve a common goal. A WSN can be expanded in harsh environments to fulfill both military and civil applications [1]. Mobile Sensor networks could be used in applications such as environment monitoring and object tracking. Recently, due to the advance in robotics, mobile sensor networks become feasible and applicable.

The small sensor nodes which are distributed over the network. These nodes sense the responsive message data from the location and send the responsive message to the sink node. The sink node will verify the data and its ID which is send by the sensor nodes[5]. The sensor nodes are expand in hostile environment and the nodes are unattended which makes an adversary to judge the sensor nodes and make many clone of them. These clone nodes are dangerous to the network communication. These mobile sensors are used in variety of application including duplicate detection, border monitoring, and military patrols.

It generates the maximum number of attacker controlled clones around the network. The dangerous attack is the compromised node attacks
in which the adversary takes the private keying materials from a compromised node. An adversary can take the single sensor ID and make many clones of them [7].

**Related Work**

The detection Techniques, based on the detection methodologies

Detection Techniques for Static WSNs
Detection Techniques for Mobile WSNs

**Detection Techniques for Stationary WSNs:**

The static WSNs detection of node replication attack in two types as centralized and distributed techniques.

**Centralized Techniques:**

In centralized techniques the detection process every node in the network sends its location claim to sink node through its neighboring nodes. Receiving the entire location claims, the sink node checks the node IDs along their location, and if it finds two other locations with the same ID, it raises a replica node. The sink node is considered to be a powerful central which is responsible for information convergence and decision making.

**Random key pre distribution:** Random key pre distribution security schemes are well suited for use in sensor networks because of their low storage overhead. However, the security of a network using pre distributed keys can be compromised by cloning attacks. Cloning gives the adversary an easy way to build an army of replica nodes that can cripple the sensor network. Brooks proposed an algorithm that a sensor network can use to detect the existence of clones. Random Keys that are present on the cloned nodes are detected by looking at how often they are used to authenticate nodes in the network.[1]

**SET:** [2] algorithm is used to detect replicas by computing set operations of exclusive subsets in the network, using localized voting mechanism, a set of neighbor nodes can agree on the duplication of a given node that has been replicated within the neighborhood. This method fails to detect duplication nodes that are not within the same neighborhood. This algorithm is used to reduce the communication cost of the preceding approach by computing set operations of exclusive subsets in the network. SET then employs a tree structure to compute non overlapping set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. First, SET launches an Exclusive subset maximal independent set (ESMIS) algorithm which forms exclusive unit subsets among one-hop neighbors in an only one disjointed subset which are controlled by a head.

**Distributed Techniques:**

There is no essential rule exists, in distributed techniques and special detection mechanism called claimer reporter-witness frame work. Claimer reporter-witness frame work is provided in which the detection is performed by locally distributed node sending the location claim not to the sink node but to a randomly selected node called witness node.

**Detection Techniques for Static WSNs**

Centralized Techniques

- Random
- SET
- DM
- RM
- RED
- LM

Distributed Techniques

- LSM

SET: [2] algorithm is used to detect replicas by computing set operations of exclusive subsets in the network, using localized voting mechanism, a set of neighbor nodes can agree on the duplication of a given node that has been replicated within the neighborhood. This method fails to detect duplication nodes that are not within the same neighborhood. This algorithm is used to reduce the communication cost of the preceding approach by computing set operations of exclusive subsets in the network. SET then employs a tree structure to compute non overlapping set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. First, SET launches an Exclusive subset maximal independent set (ESMIS) algorithm which forms exclusive unit subsets among one-hop neighbors in an only one disjointed subset which are controlled by a head.

**Distributed Techniques:**

There is no essential rule exists, in distributed techniques and special detection mechanism called claimer reporter-witness frame work. Claimer reporter-witness frame work is provided in which the detection is performed by locally distributed node sending the location claim not to the sink node but to a randomly selected node called witness node.
Deterministic Multicast (DM): [6] DM protocol is a claimer-reporter-witness framework. It is a good example to explain claimer–reporter-witness framework. This protocol is used to improve the communication cost of the previous protocol. The claimer is a node which shares its location claim to its neighbor nodes, each neighbor node serving as a reporter. The reporter uses function to map the claimer ID to a witness node. Then the neighbor node forwards the claim to the witness. Witness will receive two different location claims for the same node ID if the adversary has replicated a node. There is a problem in Deterministic Multicast. If a replica knows the claimer’s ID and function he/she will the witness’s location. Then it compromises them before deploying his replication node.

Randomized Multicast and Line Selected Multicast (RM and LSM): [8] the first protocol is called Randomized Multicast (RM) which is a distributed node replica detection mechanism. It will select the witness of the node in randomly. The second protocol, Line-Selected Multicast (LSM), exploits the routing topology of the network to select witnesses for a node location. It utilizes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbors. Then, each neighbor node chose randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes nearest to selection locations by using geographic routing. RM protocol is high communication cost, parno et al. proposed another protocol to reduce the communication overhead and increase the probability of detection, which is called as line-selected multicast (LSM). In this protocol the location claim travel from one node to another node. If we compared with RM and LSM has a lower communication cost. It has a many drawbacks.

Randomized, Efficient and Distributed Mechanism (RED): [4,5] It combines both characteristics of DM and RM, but this protocol uses the witness chosen by pseudo-randomly on a network-wide seed to improve network performance and a distributed protocol to detect the node replication attack. This protocol consist of two steps: In first step, a random value, rand, is shared between all the nodes in the network. In second step, is the detection phase, each node broadcasts its claim ID and location to its neighboring nodes. Each and every neighbor node that hears a claim sends (with probability p) to a set of g pseudo randomly chosen network places. The pseudo random function takes as an input ID, random number, and g. Each node in the path (from claiming node to the witness destination) forwards the data to its neighbor closest to the destination. It protects the witness nodes. The replicated node will be detected in every detection phase.

Localized Multicast: [15] there are two distributed protocols for detecting node replication attacks called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In both protocols, the overall Sensor network is split into cells to form a geographic grid. In SDC, every node ID is exclusively mapped to one of the cells in the grid. When executing detection method, every node broadcasts a location claim to its neighbor’s node. Then, every neighbor forwards the location claim with a probability to an exclusive cell by executing a geographic hash function with the input of node ID. Once a location claim received by the destination cell by any node, the location claim is flooded by the entire cell. Since the location claims of clone nodes will be forwarded to the same cell, hence the clone nodes will be detected with certain probability. Like SDC, in the P-MPC algorithm,
geographic hash function is employed to map node identity to the destination cells. However, instead of mapping to single deterministic cell, in P-MPC the location claim is mapped and forwarded to multiple deterministic cells with different probabilities. The rest of the process is similar to SDC.

**DETECTION TECHNIQUES FOR MOBILE WSNS:**

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.

**Centralized Techniques:**

1. **Sequential Probability Ratio Test (SPRT):** [13] 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. **Extremely Efficient Detection (XED):** [13] 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, j and i meets again and again, i can assertion whether 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

**Distributed Techniques:**

- eXtremely Efficient Detection (XED): [13] 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, j and i meets again and again, i can assertion whether 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. In online step if one u encounter v for the first time, u node randomly generates $\alpha$ ,computes $h(\alpha)$, sends $h(\alpha)$ to v .

2. Efficient and Distributed Detection of Node: [13] 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.

Conclusion:

This paper reviewed the various algorithms for detection of node replication attack. The existing systems are categorized into two techniques distributed and centralized. Both classes of algorithms experienced in detecting and preventing replica attacks, but both algorithms also have some drawbacks. However, the current study features the fact that there are still a lot of challenges and issues in replica detection algorithms.

REFERENCES:


