ISSN 2250-3153

Mobile Node Replication Attack Detection in Wireless Sensor Network

Mrs. Snehal Y. Kulkarni*, Prof. Ms. Nalini A. Mhetre**

*M. E. (Second Year), Department of Computer Engineering, Smt. Kashibai Navale College of Engg, University of Pune, India
** Assistant Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engg, University of Pune, India

Abstract- In wireless sensor network, an attacker can capture sensor nodes and can compromise sensor nodes. Then would create duplicate nodes and built up various attacks using duplicate nodes, inserts into the network. This is happened because of unattended nature of wireless sensor network. These attacks helps attacker to control few more nodes to have control over the network. There are many node replication attack detection methods which have been used to secure from attacks in the sensor network where nodes are static. These methods are dependent on fixed location of sensors and hence do not works for sensor network where nodes are mobile. In wireless sensor network where sensor node are moving i.e. mobile, for node replication attack detection proposed system is used where attacks are detected quickly. In this method basic idea is used that mobile node never have more speed than system speed. The proposed system can detect node replication attack in effective and robust manner.

Index Terms- mobile sensor network, security, sequential analysis, mobile node attack replication

I. INTRODUCTION

The *wireless sensor network* is a collection of nodes organized into a cooperative network. Each node consists of processing capability may contain multiple types of memory, have a RF transceiver, have a power source, and accommodate various sensors and actuators. In wireless sensor network if sensor nodes are at fixed location, it called as *static wireless sensor network* and sensor nodes are *static nodes*. If sensor nodes are moving, it is called as *mobile sensor network* and sensor nodes are *mobile nodes*. Mobile nodes are small robots which are having capacity of sensing, wireless communication, and movement. Robomote is a robot that functions as a single mobile node in a mobile sensor network. It is hardware and software design. Mobile nodes are useful for application such that sensor deployment, adaptive sampling, network repair and event detection [1]. The security of mobile nodes is serious. The attacker is able to obtain and extract information of mobile node, and attacker uses this information to introduce false data, disturb network operations, and have control over network communication. In this situation attacker takes secret information from compromised node and creates greater number of attacker –controlled replica nodes which share the node's secret information and identity. The attacker spreads these replicas over entire network. With the help of single affected node, the attacker creates many replica nodes.

The requirement for mobile node is that node has software and key information to communicate in the network. The attacker – controlled nodes have secret information that allow them to appear like authorized element or member of the network. Procedures for secure sensor network communication would allow replica nodes to create shared keys with other nodes and the base station, enabling the nodes to encrypt, decrypt, and authenticate their communications as they were the collected from captured node. The attacker can use this insider position in many ways. For example attacker can monitor network traffic as per his requirement. Also he could jam genuine signals from authorized nodes or inserts fake data to corrupt the sensors' monitoring operation. A more destructive attacker could use common network protocols, including cluster information, localization and data aggregation, which cause continuous disruption to network operation. Through these methods attacker who is having large number of replica nodes can easily beat the main purpose of the deployed network. Hardware solution is tamper resistant which easy to implement but it is time consuming method.

For static sensor network, many different node replication attack detection schemes are used. The primary method used by these schemes is to have node creates report of location claims which identifies its position and attempt to detect conflicting reports that signal one node in multiple locations. This approach requires fixed node location. Thus main challenge is to design a scheme which detects mobile node replication attack in effective and robust manner for mobile sensor network [3][4]. In the proposed system basic concept which used is that an original mobile node is moving at speed less than the system maximum speed. If mobile node's speed is greater than maximum speed, it is possible that at least two nodes with same identity are present in the network. The sequential analysis using probability ratio test on every mobile node using null hypothesis that mobile node has not been duplicated and an alternate hypothesis that it has duplicated nodes is performed. With the help of probability and hypothesis replicated node is detected. The proposed system detects mobile node replication attack with zero false positives and negatives. This is because the probability ratio test with sequential analysis is proven to be the best mechanism in terms of number of observations to reach a decision among all sequential and non – sequential decision processes.

II. PRELIMINARIES

In this section, problem statement, assumptions for proposed system, basic requirements of the proposed scheme are described.

1) Problem Statement:

Here, problem of detecting mobile node replication attack is tackled. If mobile node is *x* then its replica node is *x*'. Mobile node *x'* having secret information and identity same as mobile node x. An attacker creates replica node *x'* as follows: He first captures the node and extracts all secret information from it. Then he prepares new node *x*', sets identity same node *x* and loads secret information of node *x* into node *x*'. There may be multiple captured and duplicated nodes.

Main goal is to detect node *x* and *x'* (or its multiple replicas) as separate entities with same identity and keys.

2) Network Assumptions:

Consider a two-dimensional *mobile sensor network* where sensor nodes freely travel in the entire network. Also assume that every mobile sensor node's movement is physically limited by the system's maximum speed. Also assume that all direct communication links between sensor nodes are bidirectional. It is assume that every mobile node is having capability of finding its location and also validating the locations of its neighboring nodes. It is also assume that the mobile nodes in the network communicate with a base station. The base station is static as long as the nodes have a way to communicate reliably to the base station on a regular basis.

3) Adversary Model :

It is assumed that an attacker may have full control over set of sensor nodes and enabling him to build up various kinds of attacks. For example, he can introduce false data into network and disturb control protocol. Moreover he can launch denial of service attacks by squeezing the signals from authorized nodes. Also assumed that attacker try to use as many duplicated nodes of original nodes in the network as will be effective for his attack. Also it is assumed that an original and replica node (or nodes) follows the Random Waypoint Mobility (RWM) model when they are moving in the network. Note that attacker could move his duplicated nodes in different patterns to discourage the scheme.

4) Robomote: Enabling Mobility

This is hardware design of the mobile sensor node. The robomote is designed to be compatible with the popular mote/tinyos platform. The robomote (Fig. 1and Fig. 2) consists of an Atmel 8535 microcontroller. This is an 8-bit AVR RISC MCU with 8k bytes of In-system programmable flash along with 512 bytes of EEPROM and 512 bytes of Internal SRAM. The microcontroller also incorporates various desirable features like programmable sleep modes and reprogramming capability. It has two motors, compass for heading and IR sensors. Each of these is described in further detail below. The robomote is complete with the addition of a mote. The mote is used as the master. All basic functionality of the robomote is exported to the mote via modular interfaces [1].

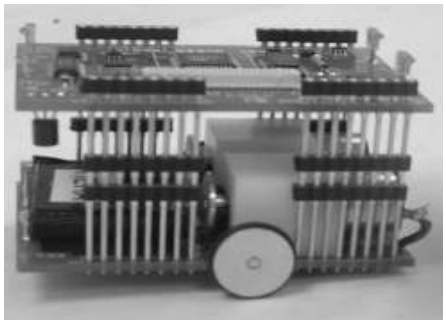

Fig 1: Robomote without the mote

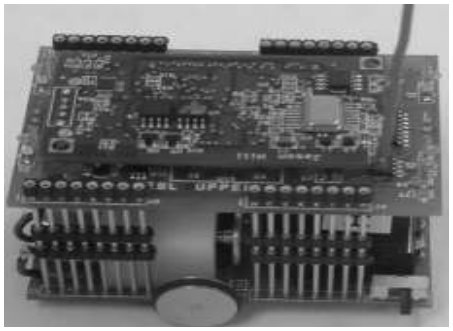

Fig 2: Robeomote with the mote

The mobile sensor node in network simulator will be as follows:

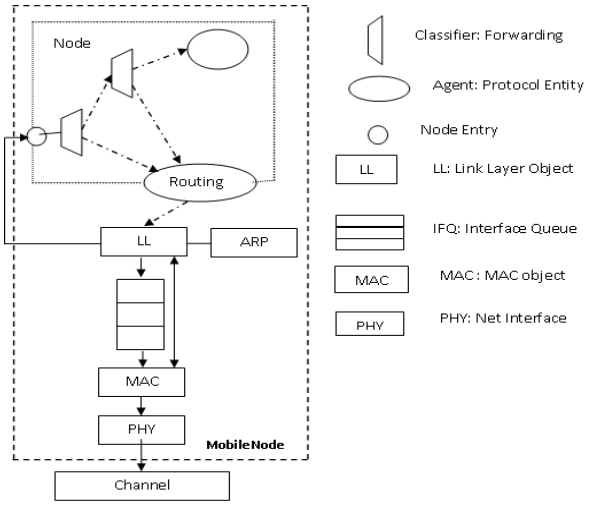

Fig. 3: Mobile node in Simulator

5) Mobility Model:

Several mobility models have been used to evaluate performance of methods which are used for detection of node replication attacks in wireless sensor network. Usually the Random Waypoint Mobility (RWM) is used. The Random waypoint model is a random-based mobility model. The mobility model is designed to describe the movement pattern of mobile nodes, and how their location. Mobility models are used for simulation purposes when new network protocols are evaluated. In the Random Waypoint Mobility model, each node moves to location which chosen randomly with speed. The speed is randomly selected with the help of a predefined minimum and maximum speed. Once reached to location, node stays at location for predefined pause time. Once pause time is completed, it then

randomly chooses another and moved to that location. The process of random movement is continuous for simulation period. When the Random Waypoint Mobility model is used in simulation, it takes some time for the probability distribution of the movement of nodes to converge to a steady state distribution after the start of simulation. Furthermore, the convergence time is changed in accordance with the parameters of the mobility model and the performance of the network varies with the convergence time. Thus, it is hard to find a steady-state distribution in the RWM model.

To resolve this problem, the Random Trip Mobility (RTM) model is proposed as a generic framework for finding the steady-state distribution of any mobility model based on random movement. It is believed that the performance of the scheme will be more accurately evaluated under a mobility model with a steady-state distribution; accordingly, Random Waypoint Mobility model with steady-state distribution obtained from Random Trip Mobility model will be used. In proposed system Random Waypoint Mobility model is used with steady – state distribution provided by the Random Trip Mobility (RTM) model [5][6].

6) Localization Techniques:

There are many different methods for estimating location of a mobile node as well as validating the location of mobile node. Some of them are described as follows:

The *Verifiable Multilateration (VM)* technique enables a secure computation and verification of the positions of mobile devices in the presence of attackers. Here, by *secure position computation* we mean that base stations compute the correct position of a node in the presence of attacker, or that a node can compute its own position in the presence of an attacker; by *secure position verification* we mean that the base stations can verify the position reported by the node. *Multilateration* is a technique for determining the position of a (mobile) device from a set of reference points whose positions are known, based on the ranges measured between the reference points and the device. The position of the device in two (three) dimensions can be computed if the device measured its distance to three (four) reference points. As we already detailed in Section II, distance estimation techniques are vulnerable to attacks from internal and external attacks, which can maliciously modify the measured distances. Multilateration is equally vulnerable to the same set of attacks because it relies on distance estimations [2].

7) Identity Based Public Key Scheme:

Identity based public key encryption in which the public key can be an arbitrary string. In such a scheme there are four algorithms [7]:

(1) setup generates global system parameters and a master-key,
(2) extract uses the master-key to generate the private key corresponding to an arbitrary public key string ID ϵ {0, 1}*
(3) encrypt encrypts messages using the public key ID,
(4) decrypt decrypts messages using the corresponding private key.

The public key operations can be effectively implemented for static sensor nodes. And also identity based public key operations are effective in mobile sensor devices which are powerful than static in terms of power. But power consumption for public key signature and verification is less than energy consumption of movement. Thus public key scheme is practical for mobile sensor networks.

III. DETECTION OF MOBILE NODE REPLICATION ATTACK

1.1. Procedure for Detection:

In mobile sensor network as nodes are moving continuously in the network techniques for detecting duplicate nodes in static sensor network are not applicable. Mobility provides hint for solving problem of node replication attack detection that a mobile sensor node never move faster than the system maximum speed. Therefore, if we examine that the mobile node speed is over the maximum speed, and then at least two nodes with the same identity are present in the network. The proposed scheme is using this observation. It is based on the probability ratio test using sequential analysis, which is a statistical decision process. Probability ratio test using sequential analysis is the best mechanism. This test considers the random walk, null hypothesis and alternate hypothesis. The null hypothesis is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. If the walk reaches or exceeds the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively.

Probability ratio test using sequential analysis for mobile node replication attack detection problem as follows. Each time a mobile sensor node moves to a new location, each of its neighbors asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the probability test by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node; it will expedite the random walk to hit or cross the upper limit and thus lead to the base station 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 expedite the random walk to hit or cross the lower limit and thus lead to the base station accepting the null hypothesis that mobile node has not been replicated. Once the base station decides that a mobile node has been replicated, it initiates revocation on the replica nodes. The proposed system is having two phases as:

1.1.1. Location claim generation:

A mobile sensor node x moves to a new location each time. First it finds location L_x and determines neighboring node N (x). By sending neighboring node y's current time't' to node x, requests for an authenticated claim for location from node x and where node y belongs to N(x). Node x checks the validity of time't' when it is received by node x.

Let,

t' = claim receipt time at node x.
Δ = transmission delay of claim.
Si_x = signature generated by node x's private key.

If

$| t' - t | > \Delta$ then, node x ignores the request.

Otherwise node *x* generates claim for location as

$$LC_x = \{x \,||\, L_x \,||\, t \,||\, Si_x\}$$

This claim sends to neighboring node y.

On the failure of verification of claim request or node *x* denies the claim request, node *x* should be removed from N(y). Also if node *x* declares a location L_x such that distance between L_y and L_x is larger than signal range of y, then it will be removed from N(y). Each neighbor node 'y' of node *x* forwards *x*'s claim to the base station with probability p.

1.1.2. Detection and Revocation:

Once location claim is received at base station, base station verifies the legitimacy of location claim with the public key of node *x* and rejects if not authentic. Genuine claims from node *x* are LC_x^1, LC_x^2… The base station extracts location information L_x^i and time information T_i from LC_x^i.

Consider,

d_i = distance from LC_x^{i-1} at time t_{i-1} to LC_x^i at time t_i.

v_i = speed at time t_i.

Where i = 1, 2, 3, ….,.

$$v_i = (d_i / | t_i - t_{i-1} |)$$

Let S_i be the random variable that is defined as

$$S_i = \begin{cases} 0, & v_i \le V_{max} \\ 1, & v_i \le V_{max} \end{cases}$$

Where V_{max} = maximum system configured speed.

The success probability *p* is defined as

$$\Pr(S_i = 1) = 1 - \Pr(S_i = 0) = p$$

By comparing *p* with a preset threshold *p'*, to decide whether node *x* is has been duplicated or not, and which can be prepared as a hypothesis testing problem with null hypothesis and alternate hypothesis. Here need to develop a suitable sampling approach in order to prevent hypothesis testing from leading to a wrong decision. Maximum possibilities of wrong decisions should be specified to tolerate for good sampling strategy. To execute this hypothesis testing problem is prepared again as one with null hypothesis and alternate hypothesis of $p < p_0$ and $p > p_1$ such that $p_0 < p_1$ respectively. In this reformulated problem, the acceptance of null hypothesis is regarded as false negative error when $p \ge p_0$ and the acceptance of the alternate hypothesis is regarded as false positive error when $p \le p_0$. The process of making decision from these two types of errors can be prevented by defining a user – configured false positive *a'* and false negative *b'* such that false positive and false negative should not go beyond *a'* and *b'* respectively. The probability ratio test using sequential analysis is performed to make a choice about node *x* from *n* experiential samples, where a measured speed of *x* is treated as a sample.

Here define,

H_0 = null hypothesis = hypothesis that node *x* has not been replicated.

H_1 = alternate hypothesis = hypothesis that node *x* has been replicated.

L_n = log probability ratio on *n* samples.

$$L_n = ln \{ (P(S_1, S_2, …., S_n | H_1) / (P(S_1, S_2, …., S_n | H_0) \}$$

If Si is independent and identically distributed then L_n as follows,

$$L_n = \sum_{i=1}^{n} \left(ln \frac{P(Si|H1)}{P(Si|H0)} \right)$$

Consider, Ω_n = number of times that $S_i = 1$ in the *n* samples

Then , $L_n = \{ \Omega_n \, l_n (p_1 / p_0) + (n - \Omega_n) \, l_n ([1-p_1] / [1- p_0])$

Where, $p_0 = P(S_i = 1 | H_0)$, $p_1 = P(S_i = 1 | H_1)$

On the basis of log probability ratio L_n, the probability ratio test using sequential analysis for H_0 against H_1 is as follows,

- $L_n \le l_n \{ b' / (1 – a') \}$: choose H_0 and end the test
- $L_n \ge l_n \{ (1 - b') / a' \}$: choose H_1 and end the test
- $l_n \{ b' / (1 – a') \} < L_n < l_n \{ (1 - b') / a' \}$: continue the test with other observation.

If node *x* is evaluated as trusted node, the base station starts the probability ratio examination using sequential analysis with recently arrived claims from *x*. If, *x* is determined to be replicated, the base station terminates the probability ratio examination on *x* and invalidates all nodes with identity *x* from the network.

1.2. Performance Analysis

For this scheme performance is analyzed in terms of the communication, computation and storage overheads.

a) Communication overheads:

The average number of claims that are sent or forwarded by nodes in the network represents communication overheads.

Theoretically, each time a mobile node *x* receives *c* claim requests on an average at a location; it sends an average of $c \times p$ claims to the base station, where *p* is the probability that the claim is forwarded to the base station. Now consider the worst-case situation in which every mobile node receives *c* claim requests at a location and sends $c \times p$ claims to the base station at the same time. Since the average hop distance between two randomly chosen nodes is given by $O(\sqrt{N})$, where N = total number of sensor nodes. Thus communication overhead in the worst case will be $(c \times p \times N \times \sqrt{N})$. Each node's requests contain the same location information *L*. Actually *O (1)* claim per location *L* is sufficient for base station to perform replica detection. $c \times p$ can be reduced to *O(1)* by setting *p* to $k(1/c) = O(1/c)$, for some constant *k* . Thus the communication overhead in worst case can be now $O(N \times \sqrt{N})$.

b) Computation and Storage Overheads:

Computation overheads are defines as average number of public key signing and verification operations per node. The computation overhead in worst case can be *O (N)*. Every time a mobile node receives *c* claim requests on an average at a location, it needs to perform *c* signature generation operations. Similarly, each time a mobile node sends *c* claim requests on an average at a location, it needs to verify up to b signatures. In the worst case, every mobile node sends $c \times p$ claims to the base station at the same time and the base station thus needs to verify up to $c \times p \times N$ signatures. The computation overhead in worst case can be *O (N)* as c and p are constants.

The average number of claims that needs to be stored by the node is called as storage overheads. The storage overhead can be one per claim. This is because the base station stores location claims to perform the probability ratio test using sequential analysis and the sensor nodes do not require to store its own or other nodes' claims. Thus, only need to compute the number of claims that are stored by the base station. Thus *N* claims are required to be stored at base station.

IV. CONCLUSION

The proposed system is centralized approach in which base station is centralized entity. The basic idea used in proposed scheme is that a mobile node never has velocity greater than the maximum velocity of system built up. Using this idea, probability ratio test with sequential analysis is performed to detect mobile node replication attack. The proposed scheme discovers node replication attack with less number of location claims. This centralized approach is efficient than deployment knowledge because deployment knowledge is not suitable for mobile sensor network, since location changes time to time in mobile wireless sensor network. The performance of the scheme is good as compared to the other approaches. The proposed scheme detects the attack faster. The proposed system can detect node replication attack in effective and robust manner.

REFERENCES

[1] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G.S. Sukhatme, "Robomote: Enabling Mobility in Sensor Networks," Proc. Fourth IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 404-409, Apr. 2005.

[2] S. Capkun and J.P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221- 232, Feb. 2006.

[3] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

[4] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[5] J.-Y.L. Boudec and M. Vojnovi_c, "Perfect Simulation and Stationary of a Class of Mobility Models," Proc. IEEE INFOCOM, pp. 2743-2754, Mar. 2005.

[6] S. PalChaudhuri, J.-Y.L. Boudec, and M. Vojnovi_c, "Perfect Simulations for Random Trip Mobility Models," Proc. 38th Ann. Simulation Symp., Apr. 2005.

[7] D. Boneh and M.K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology CRYPTO*, 2001.

AUTHORS

First Author – Snehal Y. Kulkarni, PG Student, Sinhgad Technical Education Society's Smt. Kashibai Navale College of Engineering, University of Pune, snehalk82@gmail.com

Second Author – Prof. Nalini A. Mhetre, ME (CSE), Assistant Professor, Sinhgad Technical Education Society's Smt. Kashibai Navale College of Engineering, University of Pune, nayya1@gmail.com