Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-5, February 10, 2012

Fast and Efficient Distributed Detection of Mobile Node Replica Attacks in Wireless Sensor Network

Lakabhasanee S
Dept. of M.E Communication Systems
Anna University of Technology
Madurai Campus
E-mail: lakabasanee@gmail.com

Ramesh S
M.Tech, Dept of Computer Science
Anna University of Technology
Madurai Campus
E-mail: rameshcse@autmdu.ac.in

Abstract - In wireless sensor networks, both static and mobile nodes are deployed within the network. To detect the node replica attacks in static nodes are quite easier. In case of mobile node, unable to detect the exact location and movement of node if the node has been replicated. One of the dangerous attacks in WSN is node replication attack. By using the replica node, an adversary can capture the compromised node and make use of them to inject fake data (or) to cease the network operations. A solution to stop the replica node attacks is to prevent the adversary from extracting secret key materials from mobile nodes. Previous works rely on fixed sensor locations; hence do not work in mobile sensor networks. In this work, a fast and efficient mobile node replica detection scheme is proposed using Sequential Probability Ratio Test. SPRT assigns the maximum speed for mobile node to move around the network.

Keywords: *SPRT, Game Theoretic model.*

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs is meant to be deployed in large numbers in various environments, including remote and hostile regions, with ad-hoc communications as key. A sensor node, also known as a 'mote' is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network.

In this paper, due to the unattended nature of wireless sensor networks, an adversary can capture and compromise sensor nodes, make replicas of them, and then mount a variety of attacks with these replicas. These replica node attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network. Several replica node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. The adversary can then leverage this insider position in many ways. For example, he can simply monitor a significant fraction of the network traffic that would pass through these nodes. Alternately, he could jam legitimate signals from benign nodes or inject falsified data to corrupt the sensors' monitoring operation. A more aggressive attacker could undermine common network protocols, including cluster formation, localization, and data aggregation, thereby causing continual disruption to network operations. Through these methods, an adversary with a large number of replica nodes can easily defeat the mission of the deployed network.

II. LITERATURE REVIEW

A mechanism secure positioning of wireless devices, that we call verifiable multi lateration 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 [2].Autonomous node mobility brings with it its own challenges, but also alleviates some of the traditional problems associated with static sensor networks. We illustrate this by presenting the design of the robomote, a robot platform that functions as a single mobile node in a mobile sensor network, where the robomote was used to experimentally validate algorithms designed for next generation mobile sensor networks.[3]. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications [4].In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further [5]. To detect the node replicas in mobile sensor networks, an Efficient and Distributed Detection (EDD) scheme and its variant, SEDD, schemes can be used.[6].

III. NETWORK ASSUMPTIONS

Consider that, a two-dimensional mobile sensor network where sensor nodes freely roam throughout the network [1]. It will be assumed that every mobile sensor node's movement is physically limited by the system-configured maximum speed, V_{max} and all direct communication links between sensor nodes are bidirectional.

IV. ATTACKER MODELS

The adversary can also launch a replica node attack, which is the subject of our investigation. We assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network. We also assume that the attacker attempts to employ as many replicas of one or more compromised sensor nodes in the network as will be effective for his attacks.

V. MODULE DESCRIPTION

In static sensor networks, a sensor node is regarded as being replicated if it is placed in more than one location. If nodes are moving around in network, however, this technique does not work, because a benign mobile node would be treated as a replica due to its continuous change in location. Hence, we must use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem. Specifically, a benign mobile sensor node should never move faster than the system configured maximum speed, V_{max}. Regarding errors in the measurement of time and location, we can consider both random and systematic errors. Since speed is measured based on location and time, the errors can come from either measurement. Thus, systematic time measurement error at the requesting node is likely to result in independent errors between each location claim for the nodes being measured. Systematic location measurement error means that the measurements are not independent. However, if we assume that the measurement error is consistent and biased in one direction, then the speed of a node will be measured accurately in most cases. Random location measurement errors are more likely to lead to errors in speed measurement. Thus, for our system, we treat error from one claim to the next as random and independent for the measurement of nodes speeds.

VI. DETECTION AND REVOCATION

Upon receiving a location claim from node u, the base station verifies the authenticity of the claim with the public key of u and discards the claim if it is not authentic. To understand the basis of this sampling plan, we present how the SPRT is performed to make a decision about node u from the n observed samples, where a measured speed of u is treated as a sample. We first define the null hypothesis H0 and the alternate one H1 as follows: H0 is the hypothesis that node u has not been replicated and H1 is the hypothesis that u has been replicated.

VII.SECURITY ANALYSIS

An interesting variant of this attack, however, is to keep replicas close to each other so that the perceived velocity between their location claims is less than V_{max}. To do this, an attacker coordinates a set of replicas to respond with correct claims only to those claim requests that make it appear as a single node never moving faster than V_{max}. The attacker can have some replicas grouped closely together for this purpose; replicas that are further away must ignore claim requests or respond with false claims to avoid detection.

VIII. QUARANTINE ANALYSIS

The replica nodes must ignore a minimum number of claim requests to avoid detection, but we will configure the quarantine system to react and stop the replica node attacks when many claims are ignored.This paper describes how many observations on an average are required for the base station to make a decision as to whether a node has been replicated or not. Then, it will present the communication overhead of this scheme.The base station stores location claims in order to perform the SPRT, whereas the sensor nodes do not need to keep its own or other nodes’ claims. Thus, we only need to compute the number of claims that are stored by the base station. It defines that computation and claim storage overhead as the average number of public key signing and verification operations per node and the average number of claims that needs to be stored by a node, respectively. A game-theoretic model of claim response and quarantine defense. This model is useful to understand what the optimal attack and defense strategies are and how much the attacker’s gains are limited by the optimal defense strategy when he employs the optimal attack strategy.

IX. SIMULATION RESULTS

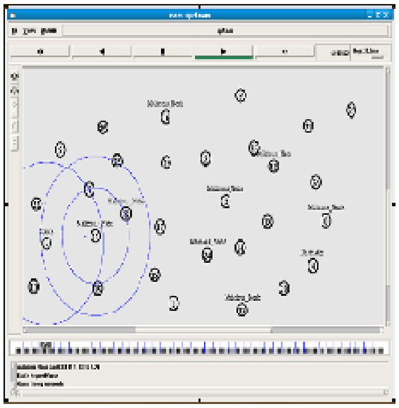

Figure 1: Route Request

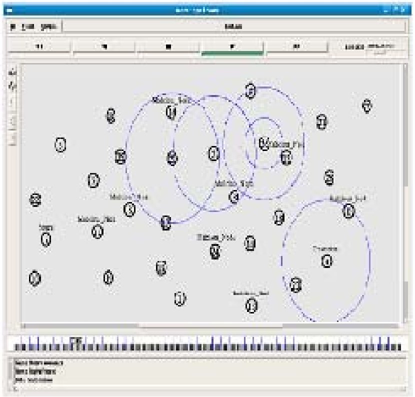

Figure 2: Route Reply

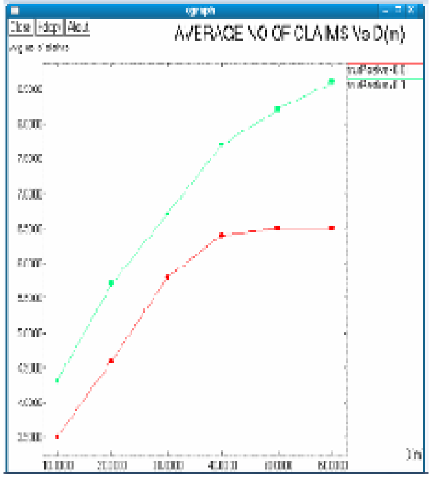

Figure 3: Average no. of Claims Vs Distance

X. CONCLUSION

A group attack strategy, in which the attacker controls the movements of a group of replicas. The quantitative analysis of the threshold values limits on the amount of time for which a group of replicas can avoid detection and quarantine. Game theoretic approach is modeled as the interaction between the detector and the adversary as a repeated game. By this way, the attacker's optimal gains are still greatly limited by the combination of detection and quarantine. I had performed simulated schemes for both static and mobile nodes in a network, where mobile nodes are expected to move. From average number of claims sent by each node had been verified by the base station, each and every node must sign their locations with their ID in the claim request, so by these claims graphical representation illustatrated the nodes had been replicated.

REFERENCES

1. Jun-Won Ho, Matthew Wright and Sajal K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing" IEEE transactions on mobile computing, vol. 10, no. 6, June 2011
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. 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.
4. J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.
5. Jing Liu, Fei Fu, Junmo Xiao and Yang Lu, "Secure Routing for Mobile Ad Hoc Networks" Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 0-7695-2909-7/07 $25.00 © 2007 IEEE.
6. G. Theodorakopoulos and J.S. Baras, "Game Theoretic Modeling of Malicious Users in Collaborative Networks," IEEE J. Selected Areas in Comm., vol. 26, no. 7, pp. 1317-1326, Sept. 2008.