Indian J.Sci.Res. 17(2): 80-84, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

IMPROVING THE QoS IN MOBILE ADHOC NETWORKS USING ENERGY EFFICIENT SCHEME

[1]A Sathiyaraj, [2]Dr. R.P.Singh, [3]N.Suvarna Parvathi lakshmi
[1]Computer Science and Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh
[2]Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh
[3]Electronics and Communication Engineering, BVC Institute of Technology and Science, Batlapalem, Amalapuram

Abstract - 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. However, these schemes rely on fixed sensor locations and hence do not work in mobile sensor networks, where sensors are expected to move. In this work, we propose a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test. To the best of our knowledge, this is the first work to tackle the problem of replica node attacks in mobile sensor networks. We show analytically and through simulation experiments that our scheme detects mobile replicas in an efficient and robust manner at the cost of reasonable overheads.

Keywords-

I. Introduction

Overview of the project

In order to protect the wireless sensor networks, particularly the replica attacks created by the adversary (hacker) can be identified using Fast Detection Method. But they are deployed in static sensors, unless the system deals with mobile dynamic sensors. An adversary can capture and compromise the nodes by making repeated replicas sequentially mounting variety of attacks on them. Earlier, schemes of literature deals with the static sensors that cannot be implemented in movable sensors.The fast and effective detection the algorithm "Sequential Probability Ratio Test (SPRT)" is used to examine the detection, in effective and also in robust manner. To tackle the problems SPRT shows the location claims to identify the adversary positions and reports. Several replica node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks.

In this proposed system deals with analytical timing and movement of adversary by a virtual image using RTMBI (Random Time Message Blocking Identifier) and RTMBP (Random Time Message Blocking Protector) techniques uses DRTG (Deterministic Random Time Generator) these techniques and algorithms shows the protection for the sensor nodes from the replica Node requests from the hackers. By the mentioned systems easily can detect and stop the adversary's replica attacks sequentially.

II. Scope Of The Project

The fast and effective mobile replica node detection scheme only by using the Sequential Probability Ratio Test. To the best of our knowledge, this is the first work to tackle the problem of replica node attacks in mobile sensor networks. The problem of positioning in wireless networks has been studied mainly in a non adversarial setting. But in this to analyze the resistance of positioning techniques to position and distance spoofing attacks. We propose a mechanism for secure positioning of wireless devices, that we call verifiable multi alteration. We then show how this mechanism can be used to secure positioning in sensor networks. We analyze our system through simulations proposed a mechanism for the secure position computation and verification of positions of wireless devices called verifiable multi alteration (VM) based on the measurements of the time of radio signal propagation. A number of indoor positioning systems were proposed, based notably on infrared ultrasound received radio signal strength and To radio signal propagation techniques These positioning techniques were then extended and used for positioning in wireless ad hoc networks.

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. However, these schemes rely on

III. Existing System

[1]Corresponding Author

fixed sensor locations and hence do not work in mobile sensor networks, where sensors are expected to move. In this scenario, a particularly dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker-controlled replicas that share the compromised node's keying materials and ID, and then spreads these replicas throughout the network.

Disadvantages:

i. The attacker use to inject fake data.

ii. Disrupt network operations

iii. Eavesdrop on network communications.

iv. The adversary can create as many replica nodes

IV. Proposed System

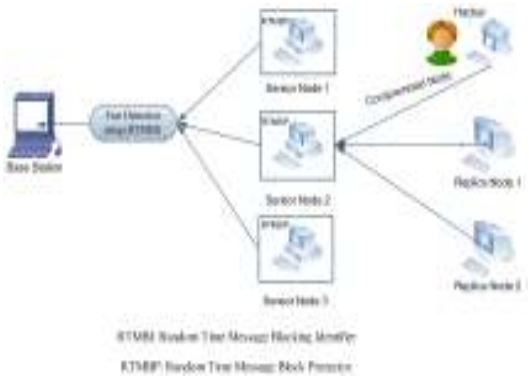
To design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks. For the effective scheme a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT) .By using the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. Also through quarantine analysis that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

Advantages:

1.Reasonable cost.

2.Report the signal one node in multiple locations.

V. System Architecture



A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design) A DFD shows what kinds of data will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

Data flow diagrams (DFDs) are one of the three essential perspectives of the structured-systems analysis and design method SSADM. The sponsor of a project and the end users will need to be briefed and consulted throughout all stages of a system's evolution. With a data flow diagram, users are able to visualize how the system will operate, what the system will accomplish, and how the system will be implemented. The old system's dataflow diagrams can be drawn up and compared with the new system's data flow diagrams to draw comparisons to implement a more efficient system. Data flow diagrams can be used to provide the end user with a physical idea of where the data they input ultimately has an effect upon the structure of the whole system from order to dispatch to report. How any system is developed can be determined through a data flow diagram. h- halftone image, α-genetic algorithm factor. This heuristic is routinely used to generate useful solutions to optimization and search problems. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover.

VI. Algorithm

The sequential probability ratio test (SPRT) is a specific sequential hypothesis test, by contrast, offers a rule of thumb for when all the data is collected (and its likelihood ratio known).

While originally developed for use in quality control studies in the realm of manufacturing, SPRT has been formulated for use in the computerized testing of human examinees as a termination criterion.

As in classical hypothesis testing, SPRT starts with a pair of hypotheses, say H_0 and H_1 for the null hypothesis and alternative hypothesis respectively. They must be specified as follows:

$$H_0: p = p_0$$

$$H_1: p = p_1$$

The next step is calculate the cumulative sum of the log-likelihood ratio, $\log\Lambda_i$, as new data arrive:

$$S_i = S_{i-1} + \log\Lambda_i$$

The stopping rule is a simple thresholding scheme:

- $a < S_i < b$: continue monitoring (*critical inequality*)
- $S_i \geq b$: Accept H_1
- $S_i \leq a$: Accept H_0

where a and b ($0 < a < b < \infty$) depend on the desired type I and type II errors, α and β. They may be chosen as follows:

$$a \approx \log \frac{\beta}{1-\alpha} \quad \text{and} \quad b \approx \log \frac{1-\beta}{\alpha}$$

In other words, α and β must be decided beforehand in order to set the thresholds appropriately. The numerical value will depend on the application. The reason for using approximation signs is that, in the discrete case, the signal may cross the threshold between samples. Thus, depending on the penalty of making an error and the sampling frequency, one might set the thresholds more aggressively. Of course, the exact bounds may be used in the continuous case.

Example

A textbook example is parameter estimation of a probability distribution function. Let us consider the exponential distribution:

$$f_\theta(x) = \theta^{-1} \exp\left(-x/\theta\right), x, \theta > 0$$

The hypotheses are simply H_0:θ = θ_0 and H_1:θ = θ_1, with $\theta_1 > \theta_0$. Then the log-likelihood function (LLF) for one sample is

$$\begin{aligned} \log \Lambda(x) &= \log \left[\frac{\theta_1^{-1} \exp\left(-x/\theta_1\right)}{\theta_0^{-1} \exp\left(-x/\theta_0\right)} \right] \\ &= \log \left[\frac{\theta_0}{\theta_1} \exp\left(x/\theta_0 - x/\theta_1\right) \right] \\ &= \frac{\theta_1 - \theta_0}{\theta_0 \theta_1} x - \log \frac{\theta_1}{\theta_0} \end{aligned}$$

The cumulative sum of the LLFs for all x is

$$S_n = \sum_{i=1}^{n} \log \Lambda(x_i) = \frac{\theta_1 - \theta_0}{\theta_0 \theta_1} \sum_{i=1}^{n} x_i - n \log \frac{\theta_1}{\theta_0}$$

Accordingly, the stopping rule is

$$b < \frac{\theta_1 - \theta_0}{\theta_0 \theta_1} \sum_{i=1}^{n} x_i - n \log \frac{\theta_1}{\theta_0} < a$$

After re-arranging we finally find

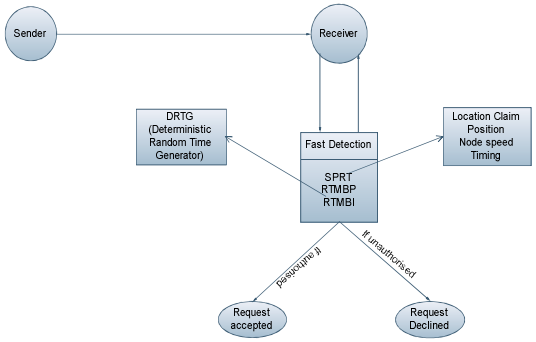
$$b + n \log \frac{\theta_1}{\theta_0} < \frac{\theta_1 - \theta_0}{\theta_0 \theta_1} \sum_{i=1}^{n} x_i < a + n \log \frac{\theta_1}{\theta_0}$$

The thresholds are simply two parallel lines with slope $\log(\theta_1 / \theta_0)$. Sampling should stop when the sum of the samples makes an excursion outside the *continue-sampling region*

DRTG Algorithm Specifications

Several DRTG mechanisms are specified in this Recommendation. The selection of a DRTG mechanism depends on several factors, including the security strength to be supported and what cryptographic primitives are available. An analysis of the consuming application's requirements for random timers should be conducted in order to select an appropriate DRTG mechanism. A detailed discussion on DRTG mechanism selection is provided. Pseudocode examples for each DRTG mechanism are provided. Conversion specifications required for the DRTG mechanism implementation is to provide security purpose maintain such illegal aspects of blocking message requests

VI. A. SPRT



If the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed. If observe that a mobile node's measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. To minimize these false positives and false negatives, to apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately. To perform the SPRT on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. In using the SPRT, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. To find that the main attack against the SPRT based scheme is when replica nodes fail to provide signed location and time information for speed measurement.

VI. B. DRTG

Deterministic Random Time Generator (DRTG), is an algorithm for generating a sequence of timings that approximates the properties of random scheduling times. The sequence is not truly random in that it is completely determined by a relatively small set generating timings, called the PRTG's state. Deterministic Random Time Generators (NRTGs). The other strategy is to Scheduling Timings deterministically using an algorithm; this class of RTGs is known as Deterministic Random

A DRTG is based on a DRTG mechanism as specified in this Recommendation and includes a source of RTMBI(Random Time Message Blocking Identifier). A DRTG mechanism uses an algorithm (a DRTG algorithm) that produces a sequence of timing for scheduling from an determined input timing to the variable accessing inputs. Once the timing is provided and the initial input throws the allocated time to variable schemes is determined, the DRTG is said to be instantiated. Because of the deterministic nature of the process, a DRTG is said to produce pseudorandom time generator, rather than random time. If the variable time is kept in secret, and the algorithm is well designed, the timed output by the DRTG will be unpredictable, up to the instantiated security strength of the DRTG. The security provided by an RTG that uses a DRTG mechanism is a system implementation issue; both the DRTG mechanism and its source of Scheduling times must be considered when determining whether the RTG is appropriate for use by consuming applications. This Recommendation specifies several diverse DRTG mechanisms, all of which provided acceptable security when this Recommendation was published. However, in the event that new attacks are found on a particular class of DRTG mechanisms, a diversity of Approved mechanisms will allow a timely transition to a different class of DRTG mechanism.

Random time generation does not require interoperability between two entities, e.g., communicating entities may use different DRTG mechanisms without affecting their ability to communicate. Therefore, an entity may choose a single appropriate DRTG mechanism for their consuming applicat

VI. C. RTMBI and RTMBP

Using these techniques and algorithms can detect the hacker Replica Node requests by assigning time to the sensors Nodes. It generates the time randomly and alternatively which cannot noticed by the Hacker. By the RTMBI technique can easily detect the requests from the adversary by DRTG generates security timings to each sensor nodes. If the request is monitored as Replica Node it decline rather accept the Base Station Node Request. The Scheme protected by the RTMBP whether any replica Nodes attack should not affect effectively. By the help of DRTG, the generator that generates the time to the sensor node at the random process.

VII. Conclusions

We have proposed a replica detection scheme for mobile sensor networks based on the SPRT. We have analytically demonstrated the limitations of attacker strategies to evade our detection technique. In particular, we first showed the limitations of a group attack strategy in which the attacker controls the movements of a group of replicas. We presented quantitative analysis of the limit on the amount of time for which a group of replicas can avoid detection and quarantine. We also modeled the interaction between the detector and the adversary as a repeated game and found a Nash equilibrium. This Nash equilibrium shows that even the attacker's optimal gains are still greatly limited by the combination of detection and quarantine. We performed simulations of the scheme under a random movement attack strategy in which the attacker lets replicas randomly move in the network and under a static placement attack strategy in which he keeps his replicas from moving to best evade detection. The results of these simulations show that our scheme quickly detects mobile replicas with a small number of location claims against either strategy

References

[1] 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.

[2] 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.

[3] J. Ho, M. Wright, and S.K. Das, "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis,"Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009

[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] L. Hu and D. Evans, "Localization for Mobile Sensor Networks,"Proc. ACM MobiCom, pp. 45-57, Sept. 2004.

[6] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan, "Fast Port scan Detection Using Sequential Hypothesis Testing," Proc.IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[7] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Seventh IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN),pp. 245-256, Apr. 2008.S

[8] 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.

[9] H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor

Networks," Ad Hoc Networks, vol. 5, no. 1,pp. 112-125, Jan. 2007.

[10] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security(CCS), pp. 264-271, Oct. 2006.

[11] 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.

[12] H. Wang, B. Sheng, C.C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, June 2008.

[13] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks," Vehicular Technology Conf. Fall (VTC Fall), Sept.2009.

[14] K. Xing, F. Liu, X. Cheng, and H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," Int'l Conf. Distributed Computing Systems (ICDCS), pp. 3-10, June 2008.