ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Sequential Probability Ratio for Detection of Mobile Replica Node Attacks in WSN

Usama Abdur Rahman[1], S. Pothumani[*2]

[1]Assistant Professor, Department of Computer Science and Engineering, Jerusalem College of Engineering, Chennai, India

[2*] Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, India

ABSTRACT: There are many replica detection schemes in the past for the static sensor networks but 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, our aim is to propose a fast and effective mobile replica node detection scheme using 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: Wireless Sensor Networks; Sequential Probability Ratio Test; Mobile Replica.

I. INTRODUCTION

Wireless sensor networks consists of a large number of sensor nodes, this sensor nodes are organized into cluster and send vital signals to the base station. This network has foreseen big changes in data gathering, processing and discriminating for monitoring specific application such as emergency services, disaster management and military applications etc.. Wireless sensor networks are application dependant. Wireless sensor network can be classified into static sensor network (ssn) and mobile sensor network (msn). In static sensor network, the sensor nodes location only first time during deployment. In case of mobile sensor network, nodes collect the data by moving from one place to another place hence localization is needed. Mobile sensor network have gained great attention in recent years due to their ability to offer economical and effective solutions in a variety of fields. There are many attacks that are prevalent in these types of sensor networks.

In potentially hostile environments, the security of unattended mobile nodes is extremely critical. An adversary takes the secret keying materials from a compromised node, and it generates a large number of attacker controlled replicas that share the compromised node's keying materials and id, and spread these replicas throughout the network. These nodes are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. It is the documentation of a comprehensive review of the published and unpublished work from secondary data sources in the areas of specific interest to the researcher.

A literature review usually precedes the proposed system and results section. Its ultimate goal is to bring the reader up to date with current literature on atopic and forms the basis for another goal, such as future research that may be needed in the area. A well-structured literature review is characterized by a logical flow of ideas; current and relevant references with consistent, appropriate referencing style; proper use of terminology; and an unbiased and comprehensive view of the previous research on the topic.

Related Works

Localized Multicast

Due to the collaborative nature of sensor nodes, time synchronization is critical for many sensor network operations. For sensor networks deployed in hostile environments, security is critical to the success of time synchronization. In the past few years, a number of secure time synchronization schemes have been proposed for sensor networks. However, these schemes are designed for homogeneous sensor networks and may incur large communication/computation overhead or cause accumulated synchronization errors (due to multi-hop relays of time reference messages). Several literatures have shown that better performance and security can be achieved in heterogeneous sensor networks (hsn). We present a secure and efficient time synchronization scheme for hsn by utilizing powerful high-end sensors. We implement the time synchronization scheme in real sensor nodes and the experiments show that our scheme achieves higher synchronization accuracy than a popular sensor time synchronization scheme. The analyses demonstrate that our scheme is resilient to various attacks and significantly reduces communication overhead.

Replication Attack Mitigations

This paper presents a novel energy-efficient mac protocol designed specifically for wireless body area sensor networks (wbasn) focused towards pervasive healthcare applications. Wireless body area networks consist of wireless sensor nodes attached to the human body to monitor vital signs such as body temperature, activity or heart-rate. The network adopts a master-slave architecture, where the body-worn slave node periodically sends sensor readings to a central master node. Unlike traditional peer-to-peer wireless sensor networks, the nodes in this biomedical wbasn are not deployed in an ad hoc fashion. Joining a network is centrally managed and all communications are single-hop. To reduce energy consumption, all the sensor nodes are in standby or sleep mode until the centrally assigned time slot. Once a node has joined a network, there is no possibility of collision within a cluster as all communication is initiated by the central node and is addressed uniquely to a slave node.to avoid collisions with nearby transmitters, a clear channel assessment algorithm based on standard listen-before-transmit (lbt) is used. To handle time slot overlaps, the novel concept of a wakeup fallback time is introduced. Using single-hop communication and centrally controlled sleep/wakeup times leads to significant energy reductions for this application compared to more “flexible” network mac protocols such as 802.11 or zigbee. As duty cycle is reduced, the overall power consumption approaches the standby power. The protocol is implemented in hardware as part of the sensium™ system-on-chip wbasn asic, in a 0.13- m cmos process.

Beyond Output Voting

Attackers routinely perform random “portscans” of ip addresses to find vulnerable servers to compromise. Network intrusion detection systems (nids) attempt to detect such behavior and flag these portscanners as malicious. An important need in such systems is prompt response: the sooner a nids detects malice, the lower the resulting damage. At the same time, a nids should not falsely implicate benign remote hosts as malicious. Balancing the goals of promptness and accuracy in detecting malicious scanners is a delicate and difficult task. We develop a connection between this problem and the theory of sequential hypothesis testing and show that one can model accesses to local ip addresses as a random walk on one of two stochastic processes, corresponding respectively to the access patterns of benign remote hosts and malicious

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

ones. The detection problem then becomes one of observing a particular trajectory and inferring from it the most likely classification for the remote host. We use this insight to develop trw (threshold random walk), an online detection algorithm that identifies malicious remote hosts. Using an analysis of traces from two qualitatively different sites, we show that trw requires a much smaller number of connection attempts (4 or 5 in practice) to detect malicious activity compared to previous schemes, while also providing theoretical bounds on the low (and configurable) probabilities of missed detection and false alarms.

Random-Walk Based Approach

Due to the unattended nature of wireless sensor networks, an adversary can capture and compromise sensor nodes, generate replicas of those nodes, and mount a variety of attacks with the replicas he injects into the network. These 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 in the literature have been proposed to defend against these attacks in static sensor networks. These approaches 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 schemes achieve effective and robust replica detection capability with reasonable overheads.

III. PROBLEM DESCRIPTION AND SPECIFICATION

Existing System

In existing system, there are many schemes for detection of replica node attacks in static sensor networks. But in mobile sensor networks, nodes are tending to move and hence locations will change so these schemes do not work on mobile sensor nodes[1].

Disadvantages

The attacker captures and compromise mobile nodes,

1. To inject fake data
2. Disrupt network operations
3. Eavesdrop on network communications.

Problem Statement

A mobile replica node having the same id and secret keying materials as original node. Adversary takes the 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[2][3].

Proposed system

In this proposed system to develop a replica detecting method for dynamic sensor network. In this network, fastly detect the mobile node replication attacks using sequential probability ratio test of the particular benign node in this network.

This project proposes a novel approach to detect the node replication attacks. The proposed approach consists of two steps which are,

1. Sprt technique
2. Defense strategy

This sequential probability ratio testing is used to detect the replication node of the mobile sensor network. This testing is applied if any one of the nodes exceeds their speed threshold of the network. Defense strategy is used to block the mobile node if it denies the claim request from their neighbor node. The proposed scheme introduces a prevention of mobile sensor nodes from the attacker by authentication key and trust-based algorithm.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

III. SYSTEM ARCHITECTURE

The term system architecture is used to describe the overall design and structure of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system[4].

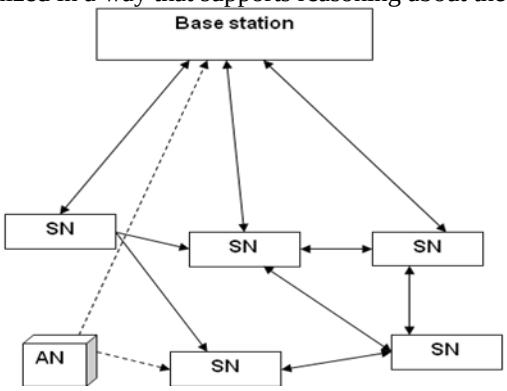


Fig 1. System architecture

In this fig(1) the group of mobile sensor nodes are controlled and monitored by the base station. The communication between these sensors is bi-directional. Each and every sensors are limited by the system configuration speed. In this network, the attacker node acts as uncompromised node to the base station[5]-[7].

Functional Architecture

The functional architecture of the proposed system is given to create a two-dimensional mobile sensor network, that every mobile sensor node's movement is physically limited by the system-configured maximum speed. All direct communication links between sensor nodes are bidirectional. A node moves to new location first it discover its neighbor node. Randomly chose its location with randomly selected speed within its maximum speed. Every mobile sensor node is capable of obtaining its location information and also verifying the locations of its neighboring nodes. To detect replica node, based on the system-configured maximum speed.

Replica nodes must ignore a minimum number of claim requests to avoid detection, but we will configure the defense strategy to react and stop the replica node attacks when many claims are ignored. A benign mobile sensor node should never move faster than the system configured maximum speed, vmax. Replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over vmax, because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds vmax, it is then highly likely that at least two nodes with the same identity are present in the network.

IV. IMPLEMENTATION

Network Configuration

To develop a network with number of mobile sensor nodes in a wireless sensor network. We consider a two-dimensional mobile sensor network where sensor nodes freely roam throughout the network. We assume that every mobile sensor node's movement is physically limited by the system-configured maximum speed, vmax. We also assume that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks.

Neighbor Node Detection

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Every mobile sensor node is capable of obtaining its distance information (random way point model). And it also assumes that the nodes in the mobile sensor network communicate with a base station. Ever sensor node to detect the neighbor node based on distance and range of network. Each time a mobile sensor node u moves to a new location, it first discovers its location lu and then discovers its set of neighboring nodes, n(u). Every neighboring node asks node u for an authenticated location claim by sending its current time t to node u. Upon receiving t, node u checks whether t is valid or not. If transmission delay of claim, and are maximum errors in time synchronization occurs, then node u will ignore the request[8][9].

Attacker Model

This module presents the details using sht (sequential hypothesis testing), this technique to detect replica node attacks in mobile sensor networks.

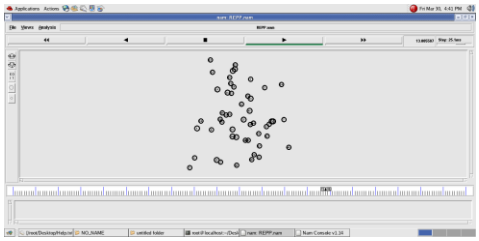
Speed denote a bernoulli random variable defined as,

S = {0; if oi < vmax; 1; if oi > vmax}

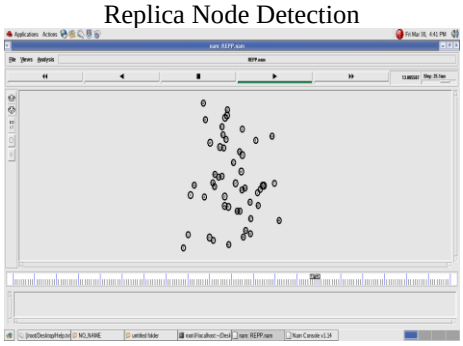
The problem of deciding whether it has been replicated or not can be formulated by hypothesis testing with null and alternate hypotheses respectively. Null hypothesis mean vmax speed controlled by system configuration, alternative hypothesis mean vmax speed increased over the system configuration. If the base station receive alternative hypothesis that node was identified attack node then the base station to black the data in that particular attack node[10][11].

V. RESULT AND EVALUATION

Movement of Nodes



Replica Node Detection

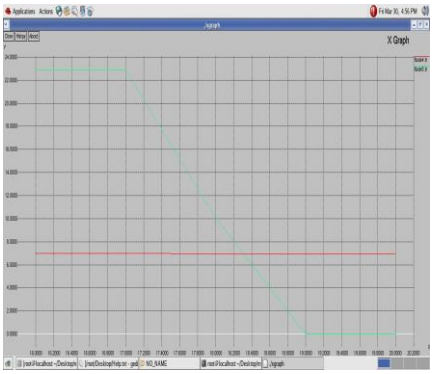


ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015



Graph Comparison between Normal Node and Replica Node Based on Speed

VI. CONCLUSION AND FUTURE WORK

In this work, 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] 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.
[2] Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
[3] 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.
[4] Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
[5] 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.
[6] Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
[7] 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.
[8] Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
[9] 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.
[10] Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
[11] 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

[12] Dr.K.P.Kaliyamurthie, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011
[13] Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013
[14] Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014
[15] P.Gayathri, Assorted Periodic Patterns Intime Series Database Usingmining, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.
[16] Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013