Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.366 – 373

RESEARCH ARTICLE

DETECTING NODE REPLICATION ATTACKS IN STATIC AND MOBILE SENSOR NETWORKS USING SPRT

T.EZHILARASAN[1]
M.Tech Student
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
ezhilarasan.mtech09@gmail.com

R.BACKIYALAKSHMI[2]
Assistant professor
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
r.backiyalakshmi@yahoo.com

ABSTRACT

Unattended nature of wireless sensor networks leads to mobile replica node attack. 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. Previous works on replica detection rely on fixed sensor locations and hence do not work in mobile sensor networks. The proposed work is a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test.

Keywords: mobile sensor network, patrol robot system, security; node replication attack, detection

I. INTRODUCTION

Security researchers have long recognized that wireless Sensor networks, with low-resource nodes that are typically left unattended and meant to be self-organizing, are potentially vulnerable to a wide range of attacks. Cryptographic protocols can prevent some attacks, such as by authenticating packets at each hop to ensure that they originate from legitimate nodes. However, an attacker can still physically capture sensor nodes, extract their cryptographic keying material, and modify their code to behave maliciously. He can also remotely compromise nodes by injecting malicious code via the exploit of certain types of software vulnerabilities With a small subset of nodes compromised through either approach, the attacker can launch a number of damaging attacks. For example, he can corrupt the monitoring operation of the base station by injecting else sensor readings, slow or stop the network by performing a distributed denial of service (DDoS) attack, or undermine critical operations such as routing, cluster formation, time synchronization, and localization.

Thus, it is very important to quickly detect and stop malicious sensor nodes to protect the sensor network and the integrity of its Operations. Prior work has investigated the detection of malicious nodes through techniques such as trace back and local misbehavior detection. These approaches are based on the assumption that the malicious activity will come from a set of fixed locations to which we can narrow our search. This assumption generally holds in static sensor networks, in which the sensor nodes do not move. This assumption can be undermined, however, by mobile malicious nodes. Although we only consider static sensor networks in this paper, the attacker could use a variety of methods to move his compromised nodes among the static nodes in the network. He could put the sensor nodes on small robots to create mobile sensors that move according to a pattern that the attacker chooses for the purpose of evading detection. Although such robotic platforms are becoming realistic and practical technology, a less sophisticated attacker with modest manpower could periodically visit each node, pick it up, and move it. Both of these methods require some additional cost, but the attacker will often be willing to incur a greater cost to avoid losing the use of his compromised nodes when they are detected. If the attacker can create mobile malicious nodes, he Will benefit from the diversification of attack paths made possible by the nodes' movements. For instance, if the attacker wishes to launch a DDoS attack against the base station, he can employ a set of mobile malicious nodes that move to as many different locations as possible and Flood the network from each location in turn. The flooding Packets can be authenticated locally but will fail to Authenticate at the base station, requiring some form of trace back to identify each attacker. In this attack scenario, however, malicious packets will traverse as many distinct paths as the number of locations that the mobile malicious nodes visit. Thus, trace back and other network- level defenses designed to find and stop immobile malicious nodes will fail. If the attacker does not target the base station, but instead aims to defeat distributed self organization protocols, such as routing and cluster formation, he can greatly raise the impact of compromising relatively few nodes by moving them around. A small group of mobile malicious nodes can disrupt these operations in one region at a time as they move around in the network, creating routing black holes, protocol failures due to time synchronization and localization errors, and other forms of havoc that otherwise would require many more compromised nodes to achieve. Local detection schemes, such as recently proposed schemes that use statistical methods to detect false data injection attacks, would not be able to collect enough data to make a decision before the mobile malicious nodes had moved away. While this also means that the region has time to recover, it will face periods of instability as the malicious nodes leave and then return to disrupt operations again. Hence, mobile malicious node attacks will have a much worse impact on the network than regular malicious node attacks.

To overcome these drawbacks, we propose a Distributed detection scheme to identify and block mobile Malicious nodes by leveraging the Sequential Probability Ratio Test (SPRT). Our scheme is designed to quickly detect and revoke mobile malicious nodes in a fully distributed manner We leverage the intuition that immobile sensor nodes appear to be present around their neighbor nodes and communicate with them regularly. On the other hand, mobile malicious nodes are absent, and therefore silent, in locations in which they previously used to be. We describe how we embed this intuition into the SPRT so that neighbors can detect and block nodes that are silent unusually often. False positives, which are an issue with any detection scheme, here only serve to remove low-value communications links between nodes that seldom communicate with each other. Our approach requires no communication overhead and very reasonable storage and computational overheads at each node.

II. NETWORK MODEL

We investigate attacks and defenses in a static (immobile) sensor network in which sensor nodes are fixed to their locations after deployment. We also assume bidirectional communication links, such that any pair of nodes that can communicate can both send and receive from each other. Moreover, we assume that sensor nodes are deployed in an automated manner. In an automated deployment, an aircraft or mobile robot randomly scatters many sensor nodes over the field. This assumption is common in sensor networks research, as it makes deployment inexpensive and manageable compared with manual deployment, especially for large networks with many nodes.

Under this assumption, researchers have addressed a variety of security problems, including key distribution, replica detection, and secure localization. Since sensor nodes cannot know their neighbor nodes before deployment, there should be a neighbor discovery period after the initial Deployment and after any redeployment, enabling each sensor node to find its neighbors. Finally, we assume that the system is using some form of trace back or local misbehavior detection. Although not necessary for our scheme to detect mobile nodes, the attacker does not need to use mobile nodes if a scheme like this is not in place to block static malicious nodes.

III. ATTACKER MODELS

We assume that an adversary may compromise and fully control a subset of the sensor nodes, enabling him to mount various kinds of attacks. For instance, he can inject false data packets into the network and disrupt local control protocols such as localization, time synchronization, and route discovery process. Furthermore, he can launch denial-of-service attacks by jamming the signals from benign nodes. However, we place some limits on the ability of the adversary to compromise nodes. We note that if the adversary can compromise major fraction nodes of the network, he will not need nor benefit much from the deployment of replicas. To amplify his effectiveness, 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. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme. We discuss this possibility in We also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor networks, because the network operator collects all sensor data and can typically control the nodes' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.

IV. MOBILE REPLICA DETECTION USING SEQUENTIAL PROBABILITY RATIO TEST

This section presents the details of our technique to detect replica node attacks in mobile sensor networks. 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, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be at most Vmax as long as we employ a speed measurement system with a low rate of error. On the other hand, 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.

We propose a mobile replica detection scheme by leveraging this intuition. Our scheme is based on the Sequential Probability Ratio Test which is a statistical decision process. The SPRT can be thought of as one dimensional random walk with the lower and upper limits before the random walk starts, null and alternate hypotheses are defined in such a way that the null hypothesis is associated with the lower limit while 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. We believe that the SPRT is well suited for tackling the mobile replica detection problem since we can construct a random walk with two limits in such a way that each walk is determined by the

observed speed of a mobile node. The lower and upper limits can be configured to be associated with speeds less than and in excess of Vmax, respectively. We apply the SPRT to the mobile replica 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 SPRT by considering speed as an observed sample. Each time the mobile node's speed exceeds (respectively, remains below) Vmax, it will expedite the random walk to hit or cross the upper (respectively, lower) limit and thus lead to the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network. Let us first describe the detection scheme and then analyze its security and performance.

V. RELATED WORKS

We first describe a number of research works on static node compromise detection in wireless sensor networks. Software attestation based schemes have been proposed to detect the subverted software modules of sensor nodes. Specifically, the base station checks whether the flash image codes have been maliciously altered by performing attestation randomly chosen portions of image codes or the entire codes.

In a sensor node's flash image codes are attested by its neighbors. However, all these schemes require each sensor to be periodically attested and thus incur a large overhead in terms of communication and computation. Our static node compromise detection scheme does not require periodic attestation but one-time attestations against untrustworthy zones. Reputation-based trust management schemes have been proposed to manage individual node's trust in accordance with its actions. Specifically, proposed a reputation-based trust management scheme in which a Bayesian formulation is used to compute an individual node's trust. Proposed information theoretic frameworks for trust evaluation. Specifically, entropy based and probability-based schemes have been proposed to compute an individual node's trust.Li et al. leveraged node mobility to reduce an uncertainty in trust computation and speed up the trust convergence. However, these trust management schemes do not revoke compromised nodes and thus compromised nodes can keep performing malicious activities in the network. Our static node compromise detection scheme revokes compromised nodes in untrustworthy zones by using software attestation technique. ID trace back schemes have been proposed to locate the malicious source of false data. However, they only trace a source of the data sent to the base station and thus they do not locate the malicious sources that send false data or Control messages to other benign nodes in the network. Our static node compromise Detection scheme does not have this limitation. We then describe some related works for mobile node compromise detection in sensor networks. A simple approach to block mobile malicious nodes is to install the list of neighboring nodes into each sensor node in the pre-deployment stage and have each node reject communications with nodes that are not included in its list. This prevents mobile malicious nodes from communicating with additional nodes or moving beyond a small area. This approach, however, requires much more work for the network operator in the pre-deployment stage, as the full topology of the network must be determined in advance. Moreover, since there are always deployment errors when using automatic deployment, it is highly likely that each node's actual neighbors are different from the pre-installed neighborhood list, causing many benign nodes to be rejected by their neighbors. It was shown in that using this simple approach leads to substantial network connectivity problems.

Location distinction schemes might be tried to detect mobile malicious nodes. In these schemes, receivers discern location changes of senders in wireless networks based on received signal strength (RSSI) or temporal radio link signatures. However, the attacker can simply turn off the node's radio during movement and move nodes far enough each time to prevent any one receiver from hearing a malicious node sending packets from two different locations. Next we present the related works for replica node detection in sensor networks. The first work on replica node detection is due to Parno et al., who proposed randomized and line-selected multicast schemes to

detect replicas in static wireless sensor networks. In the randomized multicast scheme, every node is required to multicast a signed location claim to randomly chosen witness nodes. A witness node that receives two conflicting location claims for a node concludes that the node has been replicated and initiates a process to revoke the node. The line-selected multicast Scheme reduces the communication overhead of the randomized multicast scheme by having every claim-relaying node participate in the replica detection and revocation process. Static replica detection schemes are developed for replica detection when the nodes have access to reasonable deployment knowledge. we have shown that static replica detection schemes have a number of advantages over.Contiet al. proposed a Randomized, Efficient, and Distributed (RED) protocol to enhance the line-selected multicast scheme of in terms of replica detection probability, storage and computation overheads. However, RED still has the same communication overhead as the line-selected multicast scheme of. More significantly, their protocol requires repeated location claims over time, meaning that the cost of the scheme needs to be multiplied by the number of runs during the total deployment time. Since static replica detection schemes only require claims when new nodes are deployed, they are much more efficient than RED in terms of communication overhead over the lifetime of the network.Zhu et al. proposed localized multicast schemes based on the grid cell topology, where replicas are detected by letting location claim be multicast to single cell or multiple cells. The main strength of is that it achieves higher detection rates than the best scheme of. However, have similar communication overheads as whereas static replica detection schemes work as well with much lower overheads. hoi et al. proposed a clone detection scheme in sensor networks. In this scheme, the network is considered to be a set of non-overlapping sub regions. An exclusive subset is formed in each sub region. If the intersection of subsets is not empty, it implies that replicas are included in those subsets. However, this scheme allows an adversary to bypass the detection by placing replicas in such a way that any two adjacent subsets do not include them. Static replica detection schemes can effectively address this problem. Xing et al. proposed fingerprint-based replica node detection scheme. In this scheme, nodes report fingerprints, which identify a set of their neighbors, to the base station. The base station performs replica detection by using the property that fingerprints of replicas conflict each other. Finally, we introduce the research works in which worm propagation attacks are demonstrated to be practically mounted in sensor networks and describe the related work of worm propagation prevention and the limitation of it.

Several researchers have recently showed the feasibility of malicious code injection attacks and worm propagation attacks against sensor devices. Specifically, Good speed et al. proposed a way of running malicious code on the MSP430-based TelosB motes by exploiting string format vulnerabilities and buffer overflows. Gu et al. showed that malicious code can be transiently executed on Mica2 motes and propagated to neighboring motes. Francillon et al. demonstrated that malicious code can be permanently and remotely injected into the program memory of an Atmel AVR-based sense or devices such as the MicaZ mote. They also showed that the malicious code can be easily extended to a self-propagating worm. This work is the first to break a common belief that worm propagation is impossible on sensor devices equipped with the Harvard architecture.

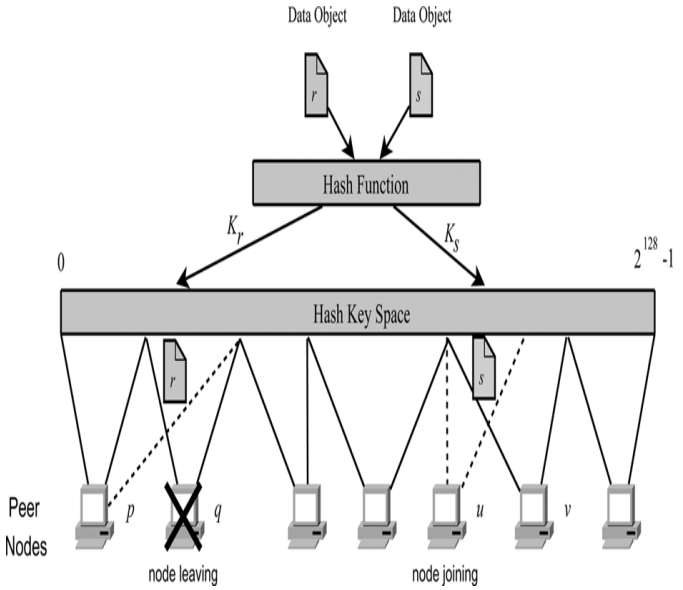
To our knowledge, there is only one work for worm propagation prevention in sensor networks. Specifically, Yang et al. used software diversity technique to prevent worm propagation in sensor networks. In this work, the network is divided into a set of grid cells and a group of sensors are deployed in each cell. Flash program is then installed into each node in such a way that all nodes in the same cell have the same version of flash program, but all nodes in a cell do not share the same version of flash program with other nodes in any adjacent cells. Even though attacker creates a worm by exploiting the vulnerability of a version of flash program assigned to a cell and infects the entire cell with that worm, he will highly likely fail to infect the adjacent cells with different versions of the flash program as long as these programs have different vulnerabilities. Hence, the main strength of this work is that it prevents a worm from propagating between two adjacent cells with little overhead. However, it is hard to automatically guarantee that different versions of flash program have different vulnerabilities. If we can discover different vulnerabilities, we can fix them and thus we do not need this scheme. On the other hand, when all versions of flash program have the same vulnerability that has not yet been identified, attacker can create a worm by

exploiting this vulnerability and infect all sensor nodes with it, leading to failure of this approach. Unlike the software diversity approach, our proposed scheme focuses on the detection of worm propagation rather than passively deterring the worm from propagating and thus does not have the aforementioned limitations.

VI. DESIGN ARCHITECTURE

A. Adversary Model:-

An adversary may compromise and fully control a subset of the sensor nodes, enabling him to mount various kinds of attacks. For instance, he can inject false data packets into the network and disrupt local control protocols such as localization, time synchronization, and route discovery process. Furthermore, he can launch denial-of-service attacks by jamming the signals from benign nodes. However, we place some limits on the ability of the adversary to compromise nodes. We note that if the adversary can compromise a major fraction node of the network, he will not need nor benefit much from the deployment of replicas. To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our investigation. It is assumed 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. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme. We also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor networks, because the network operator collects all sensor data and can typically control the nodes' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.



SYSTEM ARCHITECTURE

VII. IMPLEMENTATION

A. Normal Node

Normal node in wireless sensor network is constructed in such a way that, it has its own id and key. The sensor node forwards the data to base station. Every mobile sensor node's movement is physically limited by the system configured maximum speed.

B. Attacker Node

Attacker node is the replica node, which is created by adversary; this is known as replica node attacks. A mobile replica node u|, which has the same ID and secret key of normal mobile node u. An adversary creates replica node by first compromising node u and extracts all secret keys from it. Then prepares a new node, sets the same ID as normal node and loads normal node's secret key.

C. Claim Generation

Each and every mobile sensor node u generates location claim Cu = {u||Lu||T||Sigu} and sends it to a neighboring node v, where u, is the node identity, Lu is the Location, T is the Time and Sigu is the signature generated by node u's private key. Each time a mobile sensor node u moves to a new location, it first discovers its location Lu

D. Claim Forwarding

Base station receive location claim from the mobile sensor nodes. Upon receiving a location claim, the base station verifies the authenticity of the claim with the public key of node u and discards the claim if it is not authentic. Threshold value for the maximum velocity of the mobile sensor node is given in base station.

E. Replica Detection Using Sequential Probability Ratio Test

When a mobile sensor node moves from one location L1 to another location L2, the Euclidean distance is calculated between L1 and L2 (L2-L1). Similarly the time for the above location movement is measured using (T2-T1). Speed for a mobile sensor node is calculated using Speed S=(L2-L1)/(T2-T1). When the calculated speed S is less than the threshold, it is considered to the normal node, else it is considered to the replica node.

F.ALGORITHM (SPRT)

Step 1: Let Number of Node n, Current Location L, Current Time T
Step 2: If Node n>0, compute speed for current_location L1, current_time T1 (n) and previous_location L0 and previous time T0 (n)
Step 3: If speed >Vmax, then replica detected
Step 4: Else accept test and terminate
Step 5:Prev_loc=cur_loc
Prev_time=cur_time

CONCLUSION AND FUTUREWORK

We have proposed a replication 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 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 and also apply data structure algorithm for effective communication

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] 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] 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.

[5] 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.

AUTHORS PROFILE

Mr.T.EZHILARASAN, Presently Pursuing Final Year M.TECH CSE, In PRIST University, Pondicherry Campus, Pondicherry, India

Ms.R.BACKIYALAKSHMI, Received The M.Tech In Computer Science And Engineering. Presently she is a Working Assistant Professor in Computer Science and Engineering at PRIST University, Pondicherry Campus, and Pondicherry, India

