ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 1, January 2013

DETECTION OF NODE CAPTURE ATTACKS IN WIRELESS SENSOR NETWORKS

S.Pavaimalar[*], G.ShenbagaMoorthy[**]

[*]II-M.E, Department of CSE, A.S.L. Pauls College of Engineering and Technology, Coimbatore, India.
[**]Assistant Professor, Department of ECE, A.S.L. Pauls College of Engineering and Technology, Coimbatore, India

Abstract

Wireless Sensor Network is a collection of sensors with limited resources that collaborate in order to achieve a common goal. It is susceptible to node capture attacks because sensor nodes are deployed in unattended manner. Once opponent captures sensor nodes, he can compromise that node and launch various types of attacks with those compromised nodes. The antagonist 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. Therefore, capture node attacks are perilous and should be detected that node to reduce the harm. Several replica node detection schemes have been proposed against these attacks in static sensor networks. These approaches are worked only in static sensor network and hence do not work in mobile sensor networks. In this work, we propose a fast and effective mobile replication node detection scheme using Sequential probability Ratio Test. 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: *Sequential Analysis, Replica detection, Wireless sensor network*

I.INTRODUCTION

Wireless communication is an application of science and technology that has come to be vital for modern existence. In advance, Wireless sensor Network is used in Wireless communication for transferring the information. Wireless sensor Networks have recently gained much attention in the sense that they can be deployed for many different types of missions. In particular, they are useful for the missions that are difficult for humans to carry out. For example, they are suitable for sensing dangerous natural phenomenon such as volcano eruption, biohazard monitoring, and forest fire detection. In addition to these hazardous applications, sensor networks can also be deployed for battle field surveillance, border monitoring, nuclear and chemical attack detection, intrusion detection, flood detection, weather forecasting, traffic surveillance and patient monitoring.

To carry out a variety of missions, the network operator deploys the base station and a set of small sensor devices in the network field. Specifically, sensor devices form ad-hoc networks, collaborate with each other to sense the phenomenon associated with the assigned missions and then sends the sensory data to the base station. The network operator obtains the mission related information by analyzing the data collected at the base station. To help sensor nodes carry out the missions efficiently and effectively, many researchers proposed a variety of the network service and communication protocols. Specifically, localization, coverage, compression and aggregation protocols have been proposed for the network services. Various network protocols from physical layer to transport layer have been proposed for the communication.

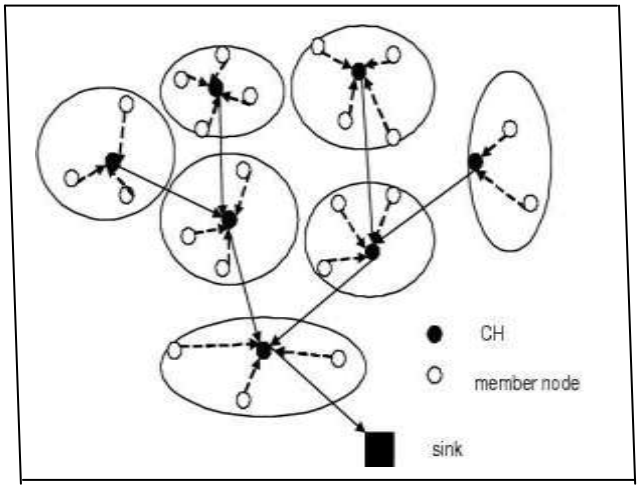

Fig.1. Sensor Network

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. For instance, an adversary could snoop on all network communications and could capture nodes thereby acquiring all the information stored in database.

However, most of them focus on making the protocols be attack-resilient rather than removing the source of attacks. Although attack-resiliency approach mitigates the threats on the network services and communication protocols, this approach requires substantial time and effort to continuously enhance the robustness of the protocols in accordance with the emergence of new types of attacks. Moreover, since it is hard to predict new types of attacks, the protocols will likely have resiliency only after being damaged by new types of attacks. Thus, we need to detect and revoke the sources of attacks as soon as possible to substantially reduce the costs and damages incurred by employing attack-resilience approach. The principle sources of various attacks are compromised sensor nodes in the sense that attacker can compromise sensor nodes by exploiting the unattended nature of wireless sensor networks and thus do any malicious activities with them.

To meet this need, we propose a node capture attack detection scheme in wireless sensor networks. We use the fact that the physically captured nodes are not present in the network during the period from the captured time to redeployed time. Accordingly, captured nodes would not participate in any network operations during that period. By leveraging this intuition, we detect captured nodes by using the Sequential Probability Ratio Test (SPRT).The main advantage of our scheme is to quickly detect captured nodes with the aid of the SPRT.

II.LITERATURE SURVEY

Sensor networks are often deployed in an unattended manner, most of these protocols are exposed to a variety of attacks such as denial of service attacks, routing disruption and false data injection attacks, network service disruption attacks (Du & Xiao, 2008; Karlof & Wagner, 2003;Wood & Stankovic, 2002). To defend the wireless sensor networks against these various attacks, many schemes have been developed in the literature. For instance, secure routing schemes have been proposed to mitigate routing disruption attacks (Karlof & Wagner,2003; Parno et al., 2006). False data injection attacks can be mitigated by using the authentication schemes (Ye et al., 2004; Yu & Li, 2009; Zhu et al., 2004). Secure data aggregation protocols are used to prevent attacker from disrupting aggregation (Chan et al., 2006; Deng et al., 2003; Przydatek et al., 2003; Yang et al., 2006). Many schemes have also been proposed to protect localization and time synchronization protocols from the threat (Capkun & Hubaux, 2006; Ganeriwal et al., 2005; Hu et al., 2008; Li et al., 2005; Liu et al., 2005; Song et al., 2007; KSun et al., 2006).A Randomized, Efficient, and Distributed (RED) protocol was proposed to enhance the line selected multicast scheme of (Parno et al., 2005) in terms of replica detection probability, storage and computation overheads (Conti et al., 2007).

However, RED still has the same communication overhead as the line-selected multicast scheme of (Parno et al., 2005). 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. Localized multicast schemes based on the grid cell topology detect replicas by letting location claim be multicast to a single cell or multiple cells (Zhu et al., 2007). The main strength of (Zhu et al., 2007) is that it achieves higher detection rates than the best scheme of (Parno et al., 2005). However, (Zhu et al., 2007) has similar communication overheads as (Parno et al.,2005).

A clone detection scheme was proposed in sensor networks (Choi et al., 2007). 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. Fingerprint-based replica node detection scheme was proposed in sensor networks (Xing et al., 2008). 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.

III. PROBLEM DEFINITION

3.1 Network Models

We first assume a static sensor network in which the locations of sensor nodes do not change after deployment. We also assume that every sensor node works in promiscuous mode and is able to identify the sources of all messages originating from its neighbors. We believe that this assumption does not incur substantial overhead because each node inspects only the source IDs of the messages from its neighbors rather than the entire contents of the messages.

3.2 Attacker Models

We assume that an attacker can physically capture sensor nodes to compromise them. However, we place limits on the number of sensor nodes that he can physically capture in each target region. This is reasonable from the perspective that an increase in the number of the captured sensor nodes will lead to a rise in the likelihood that attacker is detected by

intruder detection mechanisms. Therefore, a rationale attacker will want to physically capture the limited number of sensor nodes in each target region while not being detected by intruder detection mechanisms. Moreover, we assume that it takes a certain amount of time from capturing nodes o redeploying them in the network. This is reasonable in the sense that an attacker needs some time to compromise captured sensor nodes.

IV.PROPOSED SYSTEM

4.1 Mobile Replica Detection Using SPRT

This section presents the details of techniques to detect replica attacks in mobile sensor networks.

In static sensor networks, a sensor node can be considered to be replicated if it is placed at more than one location. However, if nodes are allowed to freely roam throughout the network, the above technique does not work because the mobile node's location will continuously change as it moves. Hence, it is imperative to use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue that can help resolve the mobile replica detection problem. Specifically, a mobile sensor node should never move faster than the system-configured maximum speed. Accordingly, if it observes that the mobile node's speed is over the maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network.

To apply 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 taking speed as an observed sample.

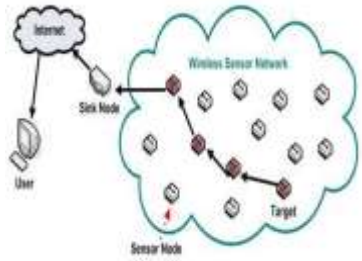

Fig .2 Detection of attacker node

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.

4.2. Protocol Description

Before deployment, every sensor node gets the secret keying materials for generating digital signatures. We will use an identity-based public key scheme such as. It has demonstrated that public key operations can be efficiently implemented in static sensor devices. Moreover, most replica detection schemes employ an identity-based public key scheme for the static sensor networks. Mobile sensor devices are generally more powerful than static ones in terms of battery power due to the fact that the mobile sensor node consumes lots of energy to move. Let d_i denote the Euclidean distance from location $Li-1u$ at time $Ti-1$ to Liu at Ti. Let o_i denote the measured speed at time Ti, where $i = 1, 2. . .$ In other words, oi is represented as:

$$oi = di/|Ti - Ti-1| \quad (1)$$

Let Si be denoting a Bernoulli random variable that is defined as:

$$Si = \begin{cases} 0, & if\ oi \le Vmax \\ 1, & if\ oi > Vmax \end{cases}$$

The success probability ↖ of Bernoulli distribution is defined as:

$$\Pr(Si = 1) = 1 - \Pr(Si = 0) = \nwarrow \quad (2)$$

Algorithm for SPRT detection

INITIALIZATION: t=1, y=0
INPUT :N_t
OUTPUT: accept the hypothesis H_o or H_1 compute s0(t) and s1(t)
if N_t ==0 **then**
y=y+1
endif
if y>=s_1(t) **then**
accept the alternate hypothesis H_1 and terminate the test
endif
if y<=s_0(t) **then**
accept the null hypothesis H_0 and initialize t t0 1 and y to 0
return;
endif
t=t+1

Additionally, the energy consumption for movement is known to be substantially larger than that for public key operations. For instance, the power consumption for the movement of a mobile sensor device was measured as 720 mW, whereas the energy consumption for public key signature is measured from 2.9 mW to 48 mW while that for public key verification was measured from 3.5 mW to 58.5 mW in accordance with the sensor hardware platforms. Thus, we believe that the public key scheme can be practical for mobile sensor networks.

We also assume that every mobile sensor node is able to obtain its location information and verify the locations of its neighboring nodes. This can be implemented by employing GPS. This assumption may not lead to additional costs if the location information is used for other purposes. Finally, we assume that the clocks of all nodes are loosely synchronized with a maximum error of. This can be achieved by the use of secure time.

V.MODULE DESCRIPTION

5.1 Network Creation

This module is developed in order to create a dynamic network. In a network, nodes are interconnected and the resources can be shared among them. For the successful data transfer the network must be properly controlled and handled. This module is designed in order to develop a controlled network traffic environment. Our project aim is to reduce the server load by splitting the server work. For these we need some replica nodes.

5.2 Identification of Replication Node

Node updates its location information to base station. At a time, both nodes send same location information to the base station of which one is true and other is false. Using the following notations it can identify the replicate node. Vmax is the configured maximum system speed and N is the Number of nodes.

5.3 Attacker Models

This section presents the details using SPRT (Sequential Probability Ratio Test), 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 had been replicated or not can be formulated as a hypothesis testing problem 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.

VI.APPLICATIONS

- Environmental magnitudes
- Gas & particle concentration
- Ambient monitoring
- Air pollution monitoring
- Forest fire detection
- Landslide detection

VII. CONCLUSION

In this paper, we proposed a node capture attack detection scheme using the Sequential Probability Ratio Test (SPRT).We showed the limitations of the benefits that attacker can take from launching node capture attacks when our scheme is employed. We also analytically showed that our scheme detects node capture attacks with a few number of samples while sustaining the false positive and false negative rates below 1%.

REFERENCES

[1] Jun-Won Ho, Mathew Wright and Sajal K.Das (2011), 'Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Sequential Hypothesis Testing', *IEEE Transactions on Mobile computing*.

[2] 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.pp. 2743-2754, Mar. 2005.

[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] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

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