IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 5 (Mar. - Apr. 2013), PP 21-26
www.iosrjournals.org

Defending Against Replication Node Attack in Wireless Sensor Network

S.Pavaimalar[1], *G.ShenbagaMoorthy*[2] , Dr.C. Kumar Charlie Paul[3]
[1]*(Department of CSE, A.S.L Pauls College of Engineering &Technology, India)*
[2]*(Department of CSE, A.S.L Pauls College of Engineering &Technology, India)*
[3]*(Department of ECE, A.S.L Pauls College of Engineering &Technology, India)*

Abstract: *In Wireless Sensor network, nodes are interconnected and information is shared among them. In a situation, many attacks are involved to misuse the wireless sensor network. One of the attacks is replica node replication attack, in which the adversary can detain and conciliation of sensor nodes by hacking IP address of node to make replicas of them and then mount a variety of attacks with these replicas. Opponent controls the entire network and misuse the whole network. Our goal is to detect and block the nodes which are captured by attacker. Sequential Probability Ratio Test is a technique which is used to find the capture node by using two approaches. However, this technique is used to detect the capture node only which affects the neighbor node and have a chance to collapse the network. Blocking Technique is needed to block the particular node captured by attacker. In this work, we propose a fast and effective method for improving the detection of node using the Black Roll technique to effectively block the node by creating a blacklist table which contains block node IP address. Protowall is a tool which is used to block the IP address that is on a blacklist table.*

Keywords-*Wireless Sensor Network, Sequential Test, Black roll, Protowall*

I. INTRODUCTION

Wireless sensor network was primarily developed as a military application to survey a battlefield. However, now a WSN is commonly used in many other industrial and commercial applications to monitor environmental conditions, health care applications and traffic controls. There are many different kinds of wireless sensor networks however; they all normally come equipped with a radio transceiver or a wireless communication device or a power source.

There are many applications to this technology and typically involve monitoring, tracking or controlling. Area monitoring comes as one very commonly used to be able to track any kind of movement whether it is heat, pressure, sound, light or vibrations in an specific area. This technology is now being utilized by almost every industry and this includes the environmentally related industry as this is a technology which allows the reading of many different kinds of changes in the atmosphere and how they can guide those in the industry to determine simple factors like water levels or more complex aspects of the environment like the possibility of an earthquake in an specific area.

Vehicle tracking and movement can also be tracked through this technology and therefore, it is also being used by the security industry. Medical science also depends on the wireless sensor network to be able to track the changes on some of the health monitors which will immediately notify the medical staff of a change in the monitoring device.

In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The attacker may be able to capture and compromise mobile nodes, and then use them to inject fake data, disrupt network operations, and eavesdrop on network communications. An adversary may replicate captured sensors and deploy them in the network to launch a variety of insider attacks. This attack process is referred to as clone attack. Mobile nodes, essentially small robots with sensing and wireless communications are useful for tasks such as static sensor deployment, adaptive sampling, network repair, and event detection. These advanced sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols.

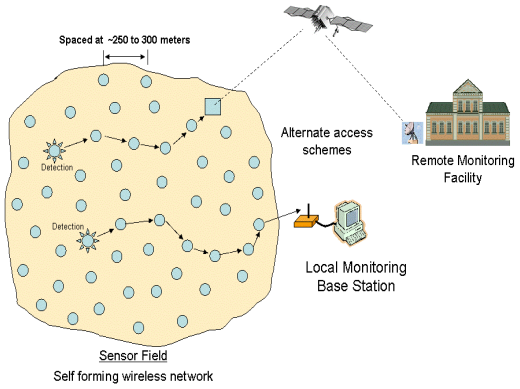

Figure 1.Wireless Sensor network

In the network, attacker capture nodes by using IP address and inject fake data to network. Misuse the network and help to enemies to collapse the network. Finally, to protect the network from adversary to provide a technique called black Roll in which to block the capture node from the other node connection.

II. PROBLEM DEFINITION

2.1 Problem Statement

We define a mobile replica node N as a node having the same ID and secret keying materials as a mobile node u. An adversary creates replica node N as follows: He first compromises node N and extracts all secret keying materials from it. Then, he prepares a new node N1, sets the ID of N to the same as u, and loads N's secret keying materials into N1.There may be multiple replicas of N, there may be multiple compromised and replicated nodes.

2.2 Network Assumptions

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. 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. 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.

III. EXISTING SYSTEM

3.1 Sequential Probability Ratio Test

This technique is the first step to block the capture node. For blocking the node, it is essential to detect the capture node by attacker. To detect the node by using Sequential Probability Ratio Test in which it provides two approaches by obtaining node's Speed. 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 we observe 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.

We apply SPRT to the mobile replica detection problem as follows. Each time a mobile sensor node moves to a new location, each of its neighbours 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. 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.

3.2 Protocol description

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.

Algorithm for SPRT detection

INITIALIZATION: n=1, y=0
INPUT :N_t
OUTPUT: accept the hypothesis H_o or H1
compute s0(t) and s1(t)
if N_t ==0 **then**
x=x+1
endif
if x>=s_1(n) **then**
accept the alternate hypothesis H_1 and terminate the test
endif
if x<=s_0(n) **then**
accept the null hypothesis H_0 and initialize n to 1 and x to 0
return;
endif
n=n+1

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. We denote the authentic claims from node u by $C^1_u, C^2_u, \ldots,$. The base station extracts location information L^i_u and time information Ti from claim C^i_u. 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:

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

The success probability ⅄of Bernoulli distribution is defined as:

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

If ⅄ is smaller than or equal to a preset threshold⅄ ′, it islikely that node *u* has not been replicated. On the contrary, if ⅄>⅄ ′, it is likely that node *u* has been replicated. The problem of deciding whether *u* has been replicated or not can be formulated as a hypothesis testing problem with null and alternate hypotheses of ⅄ ≤ ⅄*0* and ⅄ >⅄ ', respectively.

IV. PROPOSED SYSTEM

4.1 Black list table

Capture node is detected by using SPRT technique. After detect the node, the base station sends message to the server which involves capture node information like node name, address. In server, blacklist is created in it which is authenticated by using RSA algorithm. This table involves Blocking node IP address and their properties.

If a user misbehaves, the server may link any future connection from this user within the current link ability window (e.g., the same day). A user connects and misbehaves at a server during time period t within link ability window w. As part of the complaint, the server presents the nimble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods tc; tc þ 1; . . . ; tL of the same link ability window w to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day, for example (the link ability window). Note that the user's connections in t1; t2; . . . ; t_; t_ þ 1; . . . ; tc remain unlink able (i.e., including those since the misbehavior and until the time of complaint). Even though misbehaving users can be blocked from making connections in the future, the users' past connections remain unlink able, thus providing backward unlink ability and subjective blacklisting.

4.2 Protowall

To block the bad IP address to use a tool called Protowall which is a closed source freeware program for IP blocking in a network. Protowall is a lightweight program that runs in the background, taking up little CPU and memory, while blocking thousands of bad IP addresses. In Protowall, all the work is done by the driver that filters each packet, extracts the IP header and then compares the address with the ones in the table, then either discards or permits the packet to pass. The GUI is essentially a "driver instructor" that communicates to the driver the IP list to check against. The GUI also receives notifications from the driver when a packet arrives and when actions are performed with a packet. Protowall Blocks both inbound and outbound packets. Protowall blocks incoming packets from Internet addresses that are on the Blue tack Blacklists. This is handled by another program called the Block list Manager. This program finds and retrieves lists of bad IP addresses.

ProtoWall's filtering is controlled by the use of block lists, text files containing the IP addresses of organizations opposed to file-sharing . Protowall achieves this via a low-level driver that filters network traffic. It is capable of filtering all NDIS protocols including IPV6 and, most importantly, TCP/IP and UDP – two protocols which are essential for the operation of file-sharing software. The driver sits at a low-level in the system and consequently there is only a small loss of performance when the driver is active.

V. MODULE DESCRIPTION

5.1 Network Construction

Nodes are interconnected and the resources can be shared among them. Data transfer the network must be properly controlled and handled. In network Construction, two types of nodes is used. Source node is connected to the neighbor node which provides specific name and specific address. Path connection is established in between source and neighbor node in a particular network.

5.2 Key Generation

It provides authentication to node in a network to give security. Algorithm used to generate key is RSA algorithm.

Three steps of RSA algorithm are

- Key generation
- Encryption
- Decryption

RSA Algorithm

Key Generation Algorithm

- Generate two large random primes, p and q.
- Compute n = p*q and z = (p-1)(q-1).
- Choose a number relatively prime to z and call it d.
- Find e such that e*d=1 mod z.
- The public key is (n, e) and the private key is (n, d).

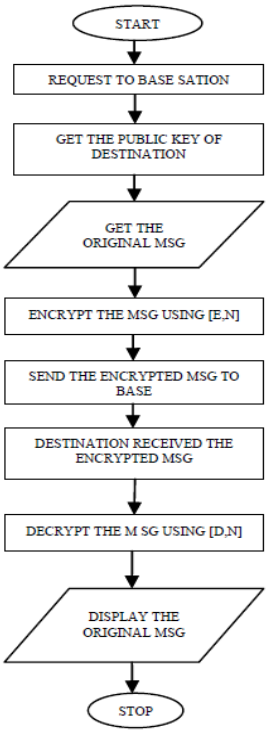

Figure 2.Flowchart

Encryption

- Sender A does the following:-
- Obtains the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer m.
- Computes the cipher text c =m^e mod n.
- Sends the ciphertext c to B.

Decryption

- Recipient B does the following:-
- Uses his private key (n, d) to compute m = c^d mod n.
- Extracts the plaintext from the integer representative m.

5.3 Attacker Model

It uses Sequential Probability Ratio Test which involves uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed (Vmax). The base station calculates the speed from all two successive claims of node.

Two approaches
1. Null Hypothesis - Node's speed is below Vmax, node has not been replicated.
2. Alternate Hypothesis - Node's speed exceedsVmax, node has been replicated.

5.4 Black Roll

Black list Table is created in server, it involves capture node information obtained from server. To provide authentication, keys are generated in table using RSA algorithm. Protowall is designed to block capture node in network. It extracts the IP header and then compares the address with the ones in the table, and then either discards or permits the packet to pass. Protowall blocks packets from Internet addresses that are on the Blacklists. It finds and retrieves lists of bad IP addresses.

VI. APPLICATIONS

- Machine health monitoring
- Industrial sense and control applications
- Preventing natural disaster
- Irrigation management
- Smart home monitoring

VII. CONCLUSION

The existing system is used for replica detection scheme for mobile sensor networks based on the SPRT. Analytical demonstration about the limitations of attacker strategies to evade the detection technique is done. In particular, the limitations of a group attack strategy in which the attacker controls the movements of a group of replicas is discussed and presented quantitative analysis of the limit on the amount of time for which a group of replicas can avoid detection and quarantine. In this paper, to propose a method to protect the network from adversary by using a technique called Black Roll which is used to block the capture node in a sensor network; it improves the detection of node replication node attacks in wireless sensor network.

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] 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.