IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 92-96
www.iosrjournals.org

Detection of Replica Nodes in Wireless Sensor Network: A Survey

Sandip D. Girase[1], Ashish T. Bhole[2]
[1,2]*Department of Computer Engineering,*
SSBT's College Of Engineering & Technology, Jalgaon, Maharashtra, India

Abstract: *Network security has become a challenging area, historically only tackled by well qualified and familiar experts. Although more pupils are becoming wired, an increasing number of pupils need to understand basics of security in the network world. The paper is written from the prospective of the basic computer user and information systems administrator, illuminating the concepts needed to go through the hype in the marketplace and understand risks and to deal with them. The replica node attacks are hazardous as they allow the attacker to leverage the compromise of a few nodes exert control over much of the network. Earlier work on replica node recognition relies on set sensor locations and hence do not work in mobile sensor network. The paper proposes sequential probability ratio test for detection of mobile replica node. It provides unique id to the sensor nodes so that an adversary can not disturb the network. The proposed sequential hypothesis testing can result in a fast and effective detection of mobile replica nodes within wireless sensor network.*

Keywords: *Wireless sensor network (WSN), network security, attack detection, node replication, tamper resistant hardware, sequential probability ratio test (SPRT)*

I. Introduction

Now a day's robotics have the advances which is responsible for developing several [1] architecture for autonomous wireless sensor networks. This unattended nature of wireless sensor networks can be exploited by adversaries. The adversaries takes the secret keying materials from a compromised node, generates a huge amount of attacker-controlled replicas that share the node's keying resources and ID, and then spreads these replicas right through the network. With a particular captured node, the adversary can form as many replica nodes as he has the hardware to generate [8]. One of the solutions for this is the use of tamper-resistance hardware to prevent adversary from extracting the keying material.

1.1 Tamper–resistant hardware

For protecting the keys the appropriate way is to store them in a tamper-resistant hardware tool. Such devices can be used for applications ranging from safe e-mail to electronic cash and credit cards. They suggest substantial shield to the keys residing within them, thus providing a few guarantee that these keys have not been maliciously read or modified. Typically in advance access to the contents of a tamper-resistant device requires knowledge of a PIN or password exactly what type of access can be gained with this knowledge is device dependent.

1.2 Sequential hypothesis test

The sequential hypothesis testing is statistical analysis where the sample size is not set in progress. as a replacement for data are evaluate as they are collected, and additional sampling is stopped in accordance with a pre-defined stopping rule as soon as significant results are observed. as a result a climax may sometimes be reached at a much earlier stage than would be possible with more classical hypothesis testing or estimation, at consequently lower financial and or individual cost.

1.3 Sequential probability ratio test

The sequential probability ratio test (SPRT) is a specific [4] sequential hypothesis test which is developed for use in quality control studies in the realm of mechanized, SPRT have been formulate used for use in the computerized testing of human examinees as a termination criterion .It is nothing but a statistical hypothesis test which is a method of making decision by means of data, whether commencing a forbidden experimentation or an observational lessons. In information, a result is called statistically significant if it is unlikely to have occurred by probability alone, according to a fixed threshold probability, the significance level. These tests are used in determining what outcomes of an experiment would lead to a rejection of the null hypothesis for a pre-specified level of significance helping to decide whether experimental results contain enough information to cast doubt on conventional wisdom. It is occasionally called assenting data investigation, in difference to investigative data analysis. Statistical hypothesis testing is a key technique of frequents

statistical inference. The critical region of a hypothesis test is the set of all outcomes which cause the null hypothesis to be rejected in support of the alternative hypothesis.

1.4 Null hypothesis

The null hypothesis is nothing but a typically corresponds to a general or default position Null hypothesis is typically paired with a subsequent assumption, the substitute hypothesis, which assert a particular relationship between the phenomena. The substitute need not be the reasonable negation of the null hypothesis it predicts the results from the experiment if the substitute assumption is true. The use of substitute hypotheses was not part of Fisher's formulation, but became standard. It is important to understand that the null hypothesis can never be expanded beyond the doubt. A set of data can only reject a null hypothesis or fail to reject it. For instance, if similarity of two groups. Null hypothesis can be work by collecting data and measuring how likely the particular set of data is, assuming the null hypothesis is true. The null hypothesis (H_0) choice and consideration of directionality is critical.

1.5 Alternative hypothesis

The alternative hypothesis (or maintained hypothesis or research hypothesis and the null hypothesis are the two rival hypotheses which are compared by a statistical hypothesis test. Sequential probability is a statistical decision process. It consists of one dimensional random walk with lower and upper limit [5]. A random walk is a mathematical formalization of a path which consists of a succession of random steps.

II. Related Work

2.1 Attack Resilient Time Synchronization in Wireless Sensor Network

In 2006, H. Song, S. Zhu, and G. Cao the time synchronization in wireless sensor network for attack resilient. In the sensor network application required time to be synchronized within the network [7]. For instance the applications include mobile object tracking, data aggregation, TDMA radio arrangement, and message ordering, to name a few. a sensor network is deployed in an area of interest to monitor passing objects which is the application of mobile object tracking. The detecting nodes record the detecting location and the detecting time, object is papering. Later, these location and time information are sent to the aggregation node which estimates the moving trajectory of the object [6]. Without accurate time synchronization, the estimated trajectory of the tracked object could differ greatly from the actual one. It also covers the network time synchronization method relay on message exchange between the nodes. Paper also gives important on the receiver –receiver model reference broadcast synchronization scheme (RBS) and its prototypes are used.

2.2 A Randomized, Efficient and Distributed Protocol

In 2007, M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, discovered the RED protocol for detection of replication attack in wireless sensor network. The randomized, efficient and distributed protocol is highly efficient as compared to other distributed protocol in the sense of communication, memory and computation [2]. In this every claim message of node is signed with its private key ,which allows other nodes to identify any malicious node not abiding to the protocol .It also allows adversary to know the witness set for any given ID. But the witness of the node will be any were in the network and it change at every protocol iteration I unpredicted way .In order to prevent RED from detecting the replicas it is required to be ubiquitous and to capture all the witness of the cloned nodes within a window period which can be at most share among the disclosure of rand and next protocol invocation. By considering adversary movement speed and realistic network size, it admires that few chances for the adversary to perform the same attack. RED performs the requirement that are area-obliviousness, ID-obliviousness ,low overhead, over head balancing and high replica attack detection probability .Consider the simulation in that n=1,000 nodes in the network, r=0.1 communication radius, g=1 and p=0.1 for the red protocol.

2.3 Distributed Detection of Node Attacks with Deployment Knowledge

The idea behind the scheme is to have nodes report location claims, which identify their positions and attempt to detect conflicting information that single one node in more than one location. For this, every node should have location claims and verify and store signed location claims of every other node .It gives the idea behind it that every node should be deploy in groups so that every node should know the information of every other node .sensors can be pre-located even if sensors can be dropped from airplanes or scattered over an area by hand (2009).Nodes are deployed in groups allow most nodes to communicate without generating any location claims as long as they are able to directly send messages to at least one of their group members. This simple idea allows us to significantly reduce the overhead of sending, receiving, and verifying location claims [1]. Additionally, if we assume loose time synchronization for the sensors, we can allow nodes to accept messages from any node that has been deployed within a small window of its expected deployment time.

2.4 Real Time Clone Detection

In 2008 K. Xing, F. Liu, X. Cheng, and H.C. Du proposed the scheme clone attack detection in wireless sensor network. In this scheme a social fingerprint is computed for each sensor by using the neighborhood characteristics, and checks the legitimacy of the originator for each message by checking the enclosed fingerprint. Generation of fingerprint is depends on the superimposed s-disjunct code, which incurs a incredibly illumination communication and computation overhead. The checking of fingerprint is conducted at both the base station as well as the nearby sensors, which ensures high detection likelihood. It also provides the real time clone detection in efficient as well as effective way. Unlimited clones were deploying by capturing and compromise nodes [3]. These nodes can be involve such as that of legitimate node and have access the legitimate IDs and keys .If these remains inside the network and left undetected then the network get unshielded to attackers and clone attackers are spread over the entire network. Smart clone may try to hide from being detected by all means. So far they may collude to cheat the network administrator into believing that they are legitimate. Clone node may be serving by adversary in the network at anywhere.

III. Proposed Work

3.1 System Architecture

Every time a mobile sensor node moves to a novel 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 or not as shown in Figure 3.1.

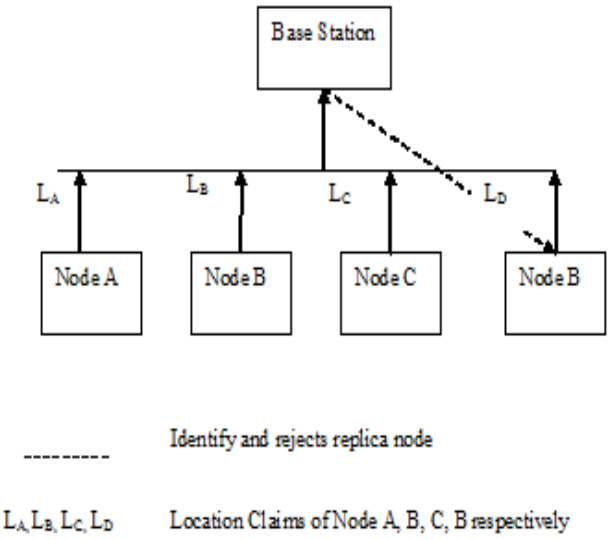

Figure 3.1: System Architecture

The base station computes the rate from every two consecutive claims of a mobile node and performs the sequential probability ratio test (SPRT) by considering speed as an observed sample. There is little benefit to the attacker of having a replica node in the same area as another compromised node. The compromised node can straightly report fake data, participate in local control protocol. Algorithm used for the proposed scheme is:

Step 1: Let the number of Nodes be n, current_locationbe L and current_time be 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 $>V_{max}$, then replica detected
Step 4: Else accept test and terminate
Step 5: Prev_loc=cur_loc
Prev_time = cur_time
Step6: Else go to step2

The flow of data for proposed scheme is shown in Figure 3.2.
Each time a mobile sensor node u moves to a new location, L_u represents the location of node u and then discovers a set of nearby nodes N (u). Each neighboring node $v \in N(u)$ asks for a true location claim from node u by sending its current time T to node u.After receiving T, node u checks whether T is valid or not. If yes then it proceed towards the location detection and finally it monitor the nodes.

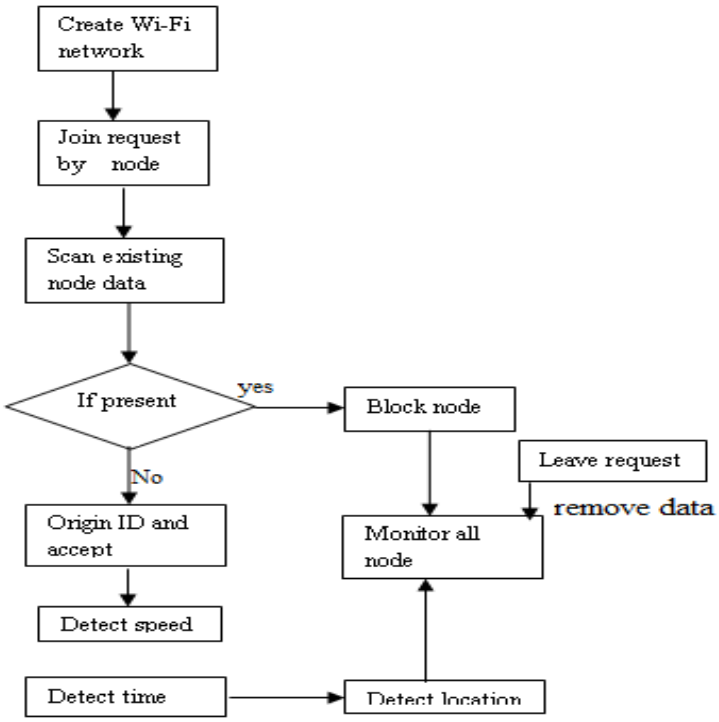

Figure 3.2: Data Flow for Proposed Work

3.2 Formulation for replica node detection and revocation

On receiving a location claim from node u, the base station verifies the authenticity of the claim with the public key of u and discards the claim if it is not genuine. We indicate the genuine claims from node u by C^1_u, $C^2_{u,}$…, $C^n_{u..}$ The base station extracts location information L^i_u and time information T_i from claim C^i_u. Let d_i denote the euclidean distance from location L^i_u at time T_i to L^{i+1}_u at T^{i+1}. Let 0_i denote the measured speed at time Ti_{+1}, where i=1, 2,…, n.

$$0_i = \frac{di}{|Ti+1-Ti|} \qquad \ldots\ldots\ldots\ldots\ldots \qquad (1)$$

Let S_i denotes a Bernoulli random variable defined as

$$S = \begin{cases} 0 \quad if 0i \le Vmax \\ 1 if\ 0i > Vmax \end{cases} \qquad \ldots\ldots\ldots\ldots\ldots \qquad (2)$$

Then, the success probability λ of the Bernouli distribution is

$$Pr(si = 1) = 1 - Pr(si = 0) = \lambda \quad \ldots\ldots\ldots\ldots\ldots \quad (3)$$

Also the log–probability ratio on η samples which is given by

$$Ln = \ln \frac{p_r(S1\ldots\ldots,Sn|\ H1)}{p_r(S1\ldots\ldots,Sn|\ H0)} \qquad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (4)$$

If S_i is independent and identically distributed, then L_n can be rewritten as

$$Ln = \ln \frac{\Pi^n_{i=1} p_r(S_i|H_1)}{\Pi^n_{i=1} p_r(S_i|H_0)} = \sum^n_i l_n \frac{P_r(S_i|H_1)}{P_r(S_i|H_0)} \ldots\ldots\ldots\ldots\ldots \quad (5)$$

Letω_n denote the number of times that S_i =1 in the n samples, we contain

$$L_n = \omega_n l_n \frac{\lambda_1}{\lambda_0} + (n - \omega_n) \ln\left(\frac{1-\lambda_1}{1-\lambda_0}\right) \ldots\ldots\ldots\ldots\ldots \quad (6)$$

Where$\lambda_0 = P_r(S_i = 1|H_0)$

The λ_0 must be configured in accord with the possibility of the occurrence that a kindly node's measured speed exceeds Vmaxdue to time synchronization and localization errors. On the other hand,$\lambda_1$should be configured to consider the possibility of the occurrence that replica nodes measured speeds exceedsVmax. While the former possibility is lower than the latter one, $\lambda_0$should be set lower thanλ_1.

IV. Conclusion

The Proposed replica node detection scheme for mobile sensor network is based on the sequential probability ratio test. It can limit the amount of time for which a group of replicas can avoid detection and quarantine. Proposed model also contain interaction between the detector and the adversary. The proposed replica node detection with sequential hypothesis testing in wireless sensor networks can quickly detect mobile replica nodes as compared to existing techniques.

References

[1]. Parno, Bryan, Adrian Perrig, and Virgil Gligor. "Distributed detection of node replication attacks in sensor networks." In Security and Privacy, 2005 IEEE Symposium on, pp. 49-63. IEEE, 2005.

[2]. Conti, Mauro, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks." In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, pp. 80-89.ACM, 2007.

[3]. Xing, Kai, Fang Liu, Xiuzhen Cheng, and David Hung-Chang Du. "Real-time detection of clone attacks inwireless sensor networks." In Distributed Computing Systems, 2008.ICDCS'08. The 28th International Conference on, pp. 3-10. IEEE, 2008.

[4]. Wald, Abraham. Sequential analysis. Courier Corporation, 1973.

[5]. Jung, Jaeyeon, Vern Paxson, Arthur W. Berger, and HariBalakrishnan. "Fast portscan detection using sequential hypothesis testing." In Security and Privacy, 2004.Proceedings. 2004 IEEE Symposium on, pp. 211-225. IEEE, 2004.

[6]. Sundararaman, Bharath, Ugo Buy, and Ajay D. Kshemkalyani. "Clock synchronization for wireless sensor networks: a survey." Ad Hoc Networks 3, no. 3 (2005): 281-323.

[7]. Song, Hui, Sencun Zhu, and Guohong Cao. "Attack-resilient time synchronization for wireless sensor networks."Ad Hoc Networks 5, no. 1 (2007): 112-125.

[8]. Choi, Heesook, Sencun Zhu, and Thomas F. La Porta. "SET: Detecting node clones in sensor networks." In Security and Privacy in Communications Networks and the Workshops, 2007.SecureComm 2007. Third International Conference on, pp. 341-350. IEEE, 2007.