International Journal of Advance Research, IJOAR .org
Volume 3, Issue 9, September 2015, Online: ISSN 2320-9194

EFFICIENT DETECTION OF MOBILE REPLICA NODE USING SEQUENTIAL ANALYSIS ON RANDOM KEY ESTABLISHMENT

V. Ram Prabha, Dr. P.Latha

1Associate Professor, VV College of Engineering, Tisaiyanvilai
prabhasuresh.v@gmail.com

2Associate Professor, Government College of Engineering, Tirunelveli

ABSTRACT

Wireless sensor network (WSN) contains a number of small sensor nodes that exchange information with other nodes through wireless medium. Since they have only restricted resources any method implemented on WSN should consider these restrictions. They habitually deployed in an environment where no monitoring is done. The dangerous attack in WSN is the node replication attack, because if any node is compromised then the same node can be replicated and it can launch a variety of attacks with the help of that node. Certain schemes have been proposed for the detection of node replication attack. Most of the schemes work for static sensor networks. Only some schemes provide solution for mobile sensor network where the sensor nodes are expected to move. We propose a method for mobile sensor networks using sequential analysis on random key establishment which efficiently identify the replicas with minimum communication overhead and minimum storage. Our simulation results show that our scheme provides better detection accuracy.

Keywords :

Wireless Sensor Network, Intrusion Detection System, Sequential Analysis, Random Key, Replica Node

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of a number of small sensor nodes deployed on a selected field. The wireless sensor nodes collect the information from their deployment area and transfer that information to the base station (BS) [1]. The architecture of a wireless sensor network is shown in the figure 1.

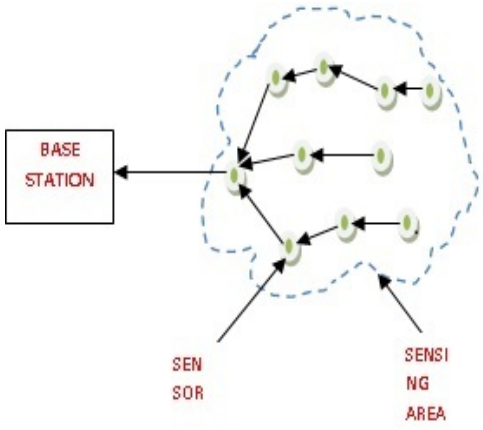

Figure 1 Architecture of WSN

A sensor node normally contains 4 basic elements which are a) sensing subsystem for collecting the data, b) processing subsystem for processing the data c) wireless communication subsystem for transmitting the processed data and d) energy subsystem for providing energy [1]. Wireless sensor networks have been applied in various applications and security in wireless sensor networks has turn into an critical issue [2]. Security issues in wireless sensor networks (WSNs) have received great interest in various fields such as medical and industry. The small sensor nodes in WSNs have limitations in computation, communication, power, and storage due to the limited resource availability. So it is a challenging task to give competent security mechanisms for WSNs [2].

There are various active attacks in which an opponent can disturb the normal operations in a wireless sensor network such as selective forwarding attack, Sybil attack, node replication attack, wormhole attack, and rushing attack, etc [3][4][5]. In a selective forwarding attack, a malicious node may purposely drop any packet and transmit the same to other ones. In the Sybil attack, a malicious node takes on multiple identities. In the node replication attack, an attacker purposely puts replicas of a compromised node in many places in the network to make discrepancy. In the wormhole attack, an opponent can tunnel packets through a secret broadband channel between two distant places and replay them to alter the network topology by making two distant nodes to believe that they are neighbours. Finally in rushing attack, an opponent can pass on route requests more rapidly than legitimate nodes so that it is more likely that the selected path include the opponent.

WSNs are habitually deployed in hostile environments without monitoring [1]. So sensor nodes can be captured and compromised easily by an opponent who may pull out the top secret information from those nodes. Compromising a legitimate sensor node may disclose essential cryptographic information and mutual secrets to the opponent. Those compromised nodes can be replicated and they can join the sensor network freely as a legitimate node. Once they join in the network they can then drastically enlarge the opponent's capacities to control the whole network maliciously. When a huge number of cloned nodes under command, the opponent may even gain control of the whole network [6]. Furthermore, the node clone will lead to most of inside attacks against sensor networks. Thus, it is important to spot clone nodes on time for minimizing their damages to WSNs.

2. RELATED WORK

Methods for detecting the replica nodes can be classified into three :

1. Methods for preventing the replica nodes from attaching with the legitimate nodes
2. Methods for detecting and revoking the replicas in centralized manner, in which a

Centralized trusted authority is responsible for finding a replica and revoke them.

3. Methods for detecting and revoking the replicas in distributed manner, in which all the nodes in the network coordinates with each other for finding the replicas and revoke them.

2.1. Methods for prevention

Zhang *et al.* [7] proposed a scheme that uses the keys which are location dependent for finding various attacks including replica node attack. The cryptographic technique based on the identity of the nodes is used. When the nodes are deployed in an area, a mobile agent move around the nodes and provide the private key for that nodes according to their identity and location. If nodes in other locations use these keys then that leads to contradiction. S. Zhu *et al.* [8] and R. Anderson *et al.* [9] proposed the schemes that uses the keys which are assigned after their deployment. These schemes based on the fact that the adversaries take some time to compromise the nodes. So the mobile agent uses this time to issue the keys for the nodes. But these schemes are location dependent and also work in static sensor networks only.

2.2.Centralized detection and revocation

The straight forward solution [10] is that the nodes send their locations and the neighbour lists to the base station which is responsible for detecting the replicas. When more than one claim contains the same ID that results in contradiction. So BS considers those nodes as replica and revoke them immediately. This scheme has several drawbacks, such as a single node failure (the BS) and high communication cost. More over the nodes nearest to the BS are transmitting more messages than the other nodes in the network. So they should need more power than the others to extend their life.

H. Choi *et al.* [11] proposed a method that minimizes the communication overhead by considering the subset of nodes such that each node belongs to exactly one subset. The information regarding the subsets is send to the base station by the leader of the subset. But this needs a protocol for forming the subsets which increase the complexity of the detection method and it works for static sensor network. Brooks *et al.* [12] proposed a scheme which is based on random key pre distribution. Every node in the network sends its key information to the base station which performs an analysis to detect the replicas. But it does not handle the situation when the malicious nodes truthfully report their keys to the base station. The centralized procedures have a drawback that they are prone to single node failure.

R. Brooks *et al.* [12] proposed a solution that considers a random key pre-distribution method. In this each and every node in the network has set of 'n' symmetric keys that are selected randomly from a pool of keys. Then a counting Bloom filter for each and every node is created based on the usage of those keys and this is send to the BS. After receiving that report the BS finds the count regarding the usage of each key in the network. When this number exceeds a particular threshold value then BS assumes that this node is replica and revokes that node from the network.

2.3.Distributed detection and revocation

Node-to-network broadcasting [13] is a simple way of detecting the replica in distributed manner. In this scheme each and every node broadcasts their location and the neighbour list which tremendously increases the communication overhead. Parno *et al.* [13] proposed two methods randomized multicast and line selected multicast. In randomized multicast random nodes are selected as special nodes and the information from the nodes is send only to the special nodes to reduce the communication overhead. In line selected multicast network topology is considered for improving the performance of the detection procedure. But this scheme is applicable to static networks and the nodes should have the details of all other node's existence which increases the storage space.

Zhu *et al.* [14] proposed a scheme which relies on a hash table to map the keys to a geographical location of the nodes. This scheme needs the knowledge of the geographical position of nodes as well as this cannot provide guarantee normally.

3 SYSTEM MODEL

In this section, we present the system, network, and adversary models considered in our system framework.

3.1 Network Model

We assume a sensor network that consists of large number of nodes that are deployed on a broad area and are moving with a predefined speed based on random way point model. The base station is a trusted one. Sensors are scattered uniformly in the network area. It is also possible to add new sensor nodes. The sensor nodes are having distinct identifier and they use pair wise public and private keys based on their identity. So the attackers cannot easily generate sensors with new identifier because they cannot generate private keys based identifiers. The public keys of the nodes are considered as their Ids. Thus no node can cheat others using their ID. Any node can check the messages sent by any other node using the sign of the sending nodes by their identity- based key. In addition to this each and every sensor node can find their geographical position and the time by a secure localization protocol and a secure time synchronization protocol. Each node can move with a system specified speed and whenever they move to a new location they need to establish a key with the new neighbours and the old neighbour list is getting erased.

3.2 Attacker Model

We took an attacker model in which the nodes are deployed in an unattended environment and they can be captured. We assume that the main aim of the attacker is to issue a node replication attack. We also assume that they can launch both passive attacks and active attacks. One such example of passive attacks and active attacks are eavesdropping on network traffic and modifying and replaying messages respectively. By the former one they can get some information which is transmitted through the network and also the time interval between communications of certain type of messages. This will be helpful for them to know the content and type of message which is transmitted over time. By the latter one they can disturb the entire network functionality. Once the nodes are compromised certain number of nodes the attacker may gain complete control over the network. But there is a restriction that the number of nodes compromised by an attacker is limited. Once some nodes are compromised by an attacker he replicates the same nodes in various places to disturb the entire network functionality. In our frame work, this replicated node is allowed to transmit messages to the other nodes as follows. The nodes that are controlled by an attacker may drop or manipulate claiming messages that they forward. The attacker can capture some nodes accordingly, but this process will take more time, and the total number of nodes that an attacker can compromise is limited. The nodes which are not controlled by the attacker will be referred as legitimate nodes. The adversary may also try to abuse a detection protocol to frame innocent nodes as cloned such that they will be expelled from the network. This is called framing attack, and approaches should be provided to address this issue.

4. DETECTING REPLICA USING SPRT AND RANDOM KEY ESTABLISHMENT

When consider a static sensor network, the detection of replica is straight forward. When two contradict claims reporting two different locations by the same node leads to the detection of replica. But this will not work in case of mobile nodes because the mobile node can be in different location at different time. We propose a mobile replica detection scheme that finds the replica efficiently. Our scheme is based on the Sequential Probability Ratio Test which can be considering as single dimensional random walk with the lower and upper bounds. The walk of mobile nodes starts from any point that lies between the two bounds and moves toward the lower or upper bound with respect to each sample. When it exceeds the lower or upper bound, it halts and according to the bound value either null hypothesis is selected or the alternate hypothesis is selected, respectively. The lower and upper are considered as the speed of a particular node in which the upper bound is the maximum configured speed as well as the maximum configured number of key establishments.

When a node ‘n’ meets its neighbour ‘m’, it establishes a random key ‘k’ with its neighbour, and maintains the count of key establishment C_{ke} with that

neighbour. When it meets the same again it checks for the count C_{ke} , If $C_{ke} > C_{th}$

Then it considers it as a replica node. Then it sends this information to the BS. Now BS applies SPRT to confirm that it is a replica node.

We assume that a genuine node moves with a speed S_{max}. So if a particular node appears in more than one place will have a moving speed greater than S_{max}. To apply the SPRT to the mobile replica detection problem as follows: Whenever a mobile node moves to a new location it has to send its claim which contains the location of the node and the time information to its neighbours. This can be done only with the newly established key whenever the node want to communicate with its neighbours. Now the old neighbour list is getting erased and the new one is getting updated. This claim along with number of key establishment is sent to the BS. Now BS checks the previous and the new claim for finding out whether the speed exceeds the maximum configured speed when taking speed as an observed sample. The BS verifies whether the count for key establishment exceeds a threshold value when taking the number of key establishment as an observed sample. Now when this happens BS sends a revocation broadcast and deletes the node from the list of nodes.

For this we have taken two hypotheses H0 and H1. H0 is the hypothesis that the node m has not been replicated and H1 is the hypothesis that the node has been replicated. We have taken the N samples and their likelihood ratio is given by

$$L_N = ln \frac{P(S1,S2,.....,SN|H1}{P(S1,S2,.....,SN|H1)}$$

Here each Sj is an independent of others. So L_N can be written as

$$L_N = ln \frac{\prod_{j=1}^{m} Pr(Sj|H1)}{\prod_{j=1}^{m} Pr(Sj|H0)} = \sum_{j=1}^{m} ln \frac{Pr(Sj|H1)}{Pr(Sj|H0)}$$

Based on this L_N the SPRT for the hypotheses H0 and H1 are as follows

- $L_N <= ln \frac{\beta'}{1-\alpha'}$: Accept H0 and stop
- $L_N >= ln \frac{\beta'}{1-\alpha'}$: Accept H1 and stop
- $ln \frac{\beta'}{1-\alpha'} < L_N < ln \frac{1-\beta'}{\alpha'}$: Continue to next step

4. RESULTS AND DISCUSSIONS

When we compare the results of both the schemes, the proposed scheme which is based on sequential analysis on number of key establishment is having the minimum communication overhead, minimum execution time and high detection accuracy.

4.1. Communication overhead and detection accuracy

First describe how many observations on an average are required for the base station to make a decision as to whether a node has been replicated or not. Then, we will present the communication overhead of our scheme. Even in speed test the nodes which are benign can also having a possibility of moving with speed which exceeds a maximum and the replica nodes can also having the possibility of moving with less speed. But in the proposed scheme definitely if a node wants to communicate then it must establish a key with it's neighbour. So the number of key establishment is definitely increased. Thus it gives high detection rate.

4.2. Computation and storage overhead

To define computation and claim storage overhead as the average number of public key signing and verification operations per node and the average number of claims that needs to be stored by a node, respectively. Each time a mobile node receives b claim requests on an average at a location, it needs to perform b signature generation operations. Similarly, each time a mobile node sends b claim requests on an average at a location, it needs to verify up to b signatures. The base station stores location claims in order to perform the SPRT, whereas the sensor nodes do not need to keep its own or other nodes' claims. Thus, we only need to compute the number of claims that are stored by the base station. In the SPRT, a sample is obtained from two consecutive location claims of node u. During an overflow, the node could stop the protocol, or drop packets to free memory. It is very important to understand what kind of impact this scenario might have on the detection capability of the protocol

itself. To summarize the above considerations with the general requirement that the overhead generated by the protocol should be small, that it should be sustainable by the WSN as a whole, and (almost) evenly shared among the nodes. every node that forwards a position claim should also perform signature verification and store the forwarded messages. As analyzed, in every line-segment includes O(√n) nodes and every node stores O(√n) location claims. It must be pointed out that this memory requirement could be impractical in real networks with thousands of nodes.

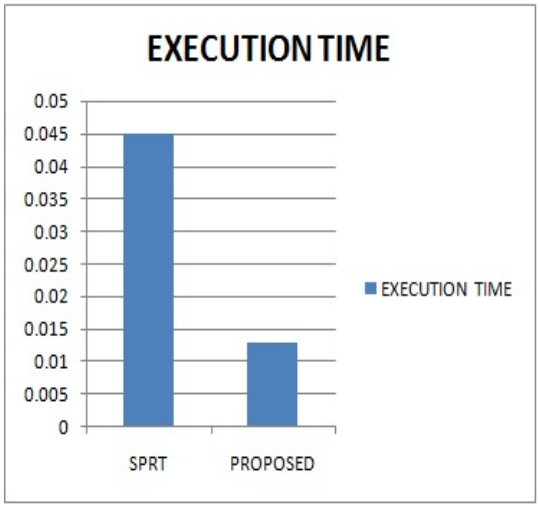

Figure 2 : Execution time analysis

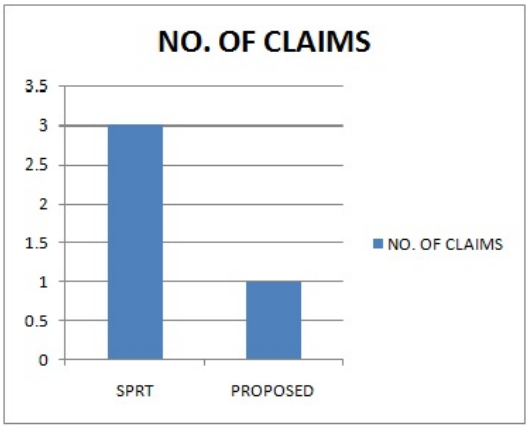

Figure 3 : No. Of claims analysis

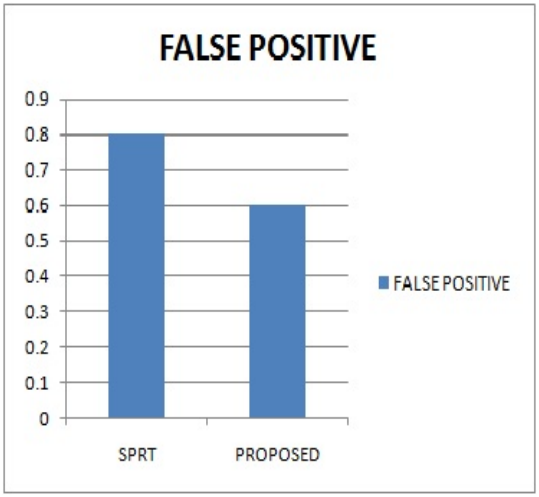

Figure 4 : False positive analysis

5. CONCLUSION

Since Wireless sensor network (WSN) contains a number of small sensor nodes and have only restricted resources, any method implemented on WSN should consider these restrictions. The dangerous attack in WSN is the node replication attack, because if any node is compromised then the same node can be replicated and it can launch a variety of attacks with the help of that node.

We propose a method for mobile sensor networks which efficiently identify the replicas with minimum communication overhead and minimum storage. We compare our results with SPRT scheme through simulation which shows that our scheme provides better detection accuracy with minimum execution time, minimum claims and low false alarm rates.

REFERENCES

[1] Ismail Butun, Salvatore D Morgera and Ravi Sankar, "A Survey of Intrusion Detection Systems in WSN", IEEE communications surveys and tutorials, 2013.

[2] Xue Deng, Renyong Wu and Wenru Wang, Renfi Bu , " An Intrusion Detection System for Cluster Based Wireless Sensor Networks", Information Technology Journal, Vol 12, no.9, pp. 1764-1771, 2013

[3]E.Cayirci and C.Rong, " Security in Wireless Adhoc and Sensor Networks", book published by Wiley, 2009

[4]G.Padmavathi and D.Shanmugapriya, " A survey of attacks, security mechanisms and challenges in Wireless Sensor Networks", International J.Computer Science, Vol 4, no.1,pp 1-9,2009

[5]A.Fuchsberger, " Intrusion Detection systems and intrusion prevention systems", Elsevier J.Information Security Technical Report, Vol 10, no.3, pp. 134-139, 2005.

[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks inwireless sensor networks,"in Proc. 8thACMMobiHoc, Montreal, QC, Canada, 2007, pp. 80–89.

[7] Y. Zhang,W. Liu,W. Lou, andY. Fang, "Location-based compromisetolerant security mechanisms for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 247–260, Feb. 2006.

[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM CCS, Washington, DC, 2003, pp. 62–72.

[9] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proc. 12th IEEE ICNP, 2004, pp. 206–215.

[10] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In CCS '02, pages 41–47, 2002.

[11] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. 3rd SecureComm, 2007, pp. 341–350.

[12] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst.s, Man, Cybern. C, Appl. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[13] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, 2005, pp. 49–63.

[14] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proc. 23rd ACSAC, 2007, pp. 257–267.