INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1456 - 1461
RECEIVED : 24/11/2016. PUBLISHED: 06/12/2016 December 6, 2016

SPRT APPROACH FOR LOCATING MRN ATTACKS IN WIRELESS SENSOR NETWORKS

[1]J.Deepak, [2]P.Manikandan, [3]S.Ragunathan, [4]V.Yamuna,
[1,2,3,4,]Assistant Professor Department of Computer Applications
AVS College of Arts & Science, Salem.

Abstract:

Nowadays Wireless sensors are playing an important role in real time applications. So security of wireless sensors is also important. Based on Random Time Stamp concept, base station can randomly change the timing in which legal nodes can communicate. Attacker nodes will not aware of this. So it will be more secure than any other methods. In the case of wireless sensor networks, an adversary can capture some legal nodes and compromise it, also make replicas of them, and mount a variety of attacks with these replicas. An uncompromised mobile node should never move at speeds in excess of the system configured maximum speed. Raising the speed threshold or other simple ways of compensating can lead to high false negative rates. To minimize these false positives and false negatives, a hypothesis testing method is used known as SPRT that can make decisions quickly and accurately. In using the SPRT, the occurrence of a speed that is exceeds the system configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. To tackle the problems, SPRT shows the location claims to identify the adversary positions and reports.

Keywords: Replica detection, sequential analysis, mobile sensor networks, security.

1. INTRODUCTION

In order to protect the wireless sensor networks, particularly the replica attacks created by the adversary (hacker) can be identified using Fast Detection Method. But they are deployed in static sensors, unless the system deals with mobile dynamic sensors. An adversary can capture and compromise the nodes by making repeated replicas sequentially mounting variety of attacks on them. To overcome this critical issue with fast and effective detection the algorithm Sequential Probability Ratio Test (SPRT) is used to examine the detection, in effective and also in robust manner. To tackle the problems SPRT shows the location claims to identify the adversary positions and reports. Proposed system deals with analytical timing and movement of adversary by a virtual image. By the mentioned systems easily can detect and stop the adversary's replica attacks sequentially Here I am proposing a concept called Random Time Stamp. In Random Time Stamp Concept, Base station will send one message to all the sensor nodes about their message transfer time. If any one of the sensor node will communicate at wrong time, then the base station can assure, that node is under the control of attacker. Attacker is misusing this legal sensor node. Based on this concept, base station can randomly change the timing in which legal nodes can communicate. Attacker nodes will not aware of this. So it will be more secure than any other methods.

2. LITERATURE REVIEW

All proposed methods about Replica Node Attacks in wireless sensor networks works only in fixed sensors. But nowadays mobile sensors are the commonly used sensors. They are expected to move in different locations depends on the real time applications. Literature survey gives an overview about these proposed systems. These are the supporting papers of my work. This literature survey extracts information from some of the literature available on this subject. It does not claim to be complete nor does it take a position towards the opinions expressed in these concepts.

All the node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, here proposes a new method.

2. SYSTEM MODEL

RANDOM TIME STAMP

Method used in this paper for detecting MRN attack is Random Time Stamp concept. In Random Time Stamp Concept, Base station will send one message to all the sensor nodes which says that “ Send message or data in between a particular timing such as 10 am-11 am,11.30 am-1pm,1.15 pm -2 pm like that. In this case all the sensor nodes which are under the control of base station should aware of this information from the base station. If any one of the sensor node will communicate at wrong time, then the base station can assure, that node is under the control of attacker. Attacker is misusing this legal sensor nodes. Based on this concept, base station can randomly change the timing in which legal nodes can communicate. Attacker nodes will not aware of this. So it will be more secure than any other methods. For detecting MRN attack Sequential Probability Ratio Test is also used. This is an approach which will detect mobile replica node attacks in wireless sensor network. 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.

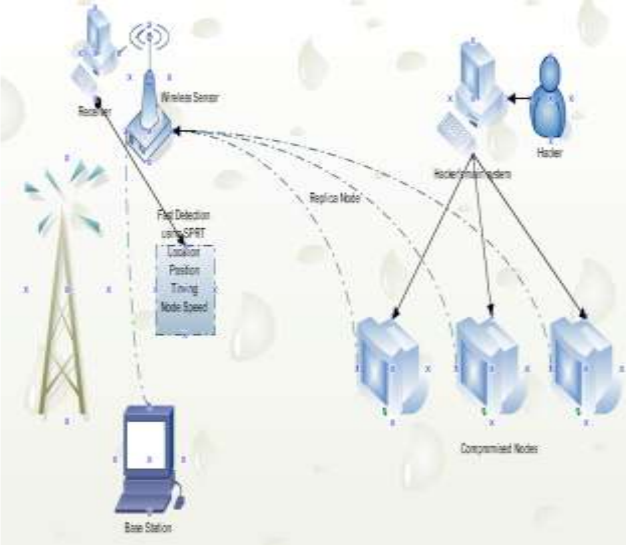

Fig.1 system architecture

If the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed. Accordingly, if we observe that a mobile node's measured speed is over the system-configured maximum speed, it is then

highly likely that at least two nodes with the same identity are present in the network. To minimize these false positives and false negatives, we apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately. We perform the SPRT on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. In using the SPRT, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica node will be revoked from the network. We find that the main attack against the SPRT based scheme is when replica nodes fail to provide signed location and time information for speed measurement.

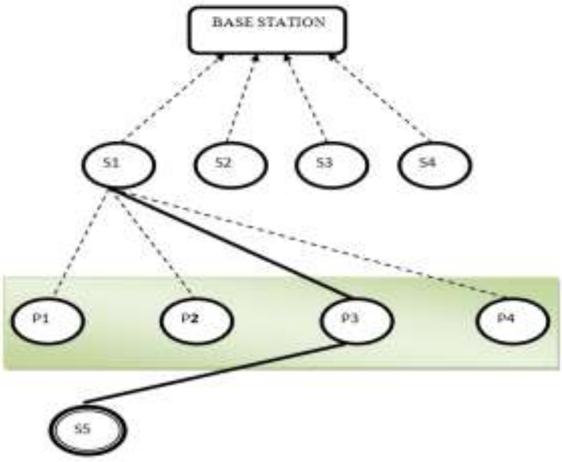

Fig.2 Working mechanism

3. ALGORITHM

The **sequential probability ratio test** (SPRT) is a specific sequential hypothesis test, by contrast, offers a rule of thumb for when all the data is collected (and its likelihood ratio known).While originally developed for use in quality control studies in the realm of manufacturing, SPRT has been formulated for use in the computerized testing of human examinees as a termination criterion.

1. As in classical hypothesis testing, SPRT starts with a pair of hypotheses, say H_0 and H_1 for the null hypothesis and alternative hypothesis respectively. They must be specified as follows

   $H_0: p = p_0$

   $H_1: p = p_1$

2. The next step is calculate the cumulative sum of the log-likelihood ratio, $\log\Lambda_i$, as new data arrive

   $S_i = S_{i-1} + \log\Lambda_i$

3. The stopping rule is a simple threshold scheme

- $a < S_i < b$: continue monitoring (*critical inequality*)
- $Si >= b$: Accept H_1
- $Si <= a$: Accept H_0

where a and b ($0 < a < b < \infty$) depend on the desired type I and type II errors, α and β. They may be chosen as follows:

$$a \approx \log \frac{\beta}{1-\alpha} \text{ and } b \approx \log \frac{1-\beta}{\alpha}$$

1. In other words, α and β must be decided before hand in order to set the thresholds appropriately. The numerical value will depend on the application.

2. The reason for using approximation signs is that, in the discrete case, the signal may cross the threshold between samples. Thus, depending on the penalty of making an error and the sampling frequency, one might set the thresholds more aggressively. Of course, the exact bounds may be used in the continuous case.

Example

A textbook example is parameter estimation of a probability distribution function. Let us consider the exponential distribution

$$f_\theta(x) = \theta^{-1} \exp\left(-x/\theta\right), x, \theta > 0$$

Equation. 2

The hypotheses are simply H_0:θ = θ$_0$ and H_1:θ = θ$_1$, with θ$_1$ > θ$_0$. Then the log-likelihood function (LLF) for one sample is

$$\begin{aligned} \log \Lambda(x) &= \log \left[\frac{\theta_1^{-1} \exp\left(-x/\theta_1\right)}{\theta_0^{-1} \exp\left(-x/\theta_0\right)}\right] \\ &= \log \left[\frac{\theta_0}{\theta_1} \exp\left(x/\theta_0 - x/\theta_1\right)\right] \\ &= \frac{\theta_1 - \theta_0}{\theta_0\theta_1} x - \log \frac{\theta_1}{\theta_0} \end{aligned}$$

Equation. 3

The cumulative sum of the LLFs for all x is

$$S_n = \sum_{i=1}^{n} \log \Lambda(x_i) = \frac{\theta_1 - \theta_0}{\theta_0\theta_1} \sum_{i=1}^{n} x_i - n \log \frac{\theta_1}{\theta_0}$$

Equation. 4

Accordingly, the stopping rule is

$$b < \frac{\theta_1 - \theta_0}{\theta_0\theta_1} \sum_{i=1}^{n} x_i - n \log \frac{\theta_1}{\theta_0} < a$$

Equation. 5

After re-arranging we finally find

$$b + n\log\frac{\theta_1}{\theta_0} < \frac{\theta_1 - \theta_0}{\theta_0\theta_1}\sum_{i=1}^{n} x_i < a + n\log\frac{\theta_1}{\theta_0}$$

4. IMPLEMENTATION RESULT

This scheme specifically for mobile sensor networks. Based on this concept, base station can randomly change the timing in which legal nodes can communicate. Attacker nodes will not aware of this. So it will be more secure than any other methods. Detects mobile replicas in an effective and robust manner with reasonable overheads. It will prevent the extraction of secret key materials from mobile nodes.

CONCLUSION

This system proposed a replica detection scheme for mobile sensor networks based on the Random Time Stamp concept. Random Time Stamp concept will be more secure than any other methods. This scheme specifically for mobile sensor networks. SPRT is the fastest scheme for the mobile replica node detection. By implementing this mechanism, the system can easily detect that which is benign node in the network and also the current position of the attacking replica node. To overcome the critical issues related with fast and effective detection, the algorithm "Sequential Probability Ratio Test (SPRT)" is used in effective and also in robust manner. Here modeled the interaction between the detector and the adversary as a repeated game like trial and error method. The result shows that even the attacker's optimal gains are still greatly limited by the combination of detection and quarantine. This scheme proposed 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. Conclusion of this paper shows that, this is a fast and effective method for MRN attacks with less overhead and high accuracy.

REFERENCES

[1] A. Wald, Sequential Analysis. Dover, 2004.

[2] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[3] H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1,pp. 112-125, Jan. 2007.

[4] H. Wang, B. Sheng, C.C. Tan, and Q. Li, "Comparing Symmetric- Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, June 2008.

[5] 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.

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

[7] 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.

[8] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, “TinySeRSync: Secure and Resilient Time Synchronization in Wireless Sensor Networks,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS), pp. 264-271, Oct. 2006.

[9] 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.

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

[11] 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.

[12] 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.