International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 9 (September 2014), PP.54-59

Novel Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Reputation Based Data Validation

A.P.V.Raghavendra[1], S.Belinsha[2]
[1]*Department of Computer Science and Engineering, V.S.B Engineering College Karur, India*
[2]*Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, India*

Abstract:- An attacker can capture and compromise sensor nodes, takes the confidential information from sensor nodes and create various attacks with these replicas. An adversary can create mobile replicas of sensor nodes, to transmit fake data, to handle and control the network operations. The Sequential Probability Ratio Test (SPRT) and quarantine defense strategies were proposed to detect and optimise mobile replicas in wireless sensor networks. The detection of replica node is based on mobility of nodes, where the sensor nodes and the mobile replica have the same mobility; it's difficult to find replicas in sensor networks. In order to find mobile replica in sensor networks, we propose reputation based data validation scheme to tackle the problem of replica node attacks. Finally, the proposed scheme detects mobile replicas in an efficient and robust manner through the simulation results.

Keywords:- Replica detection, SPRT, mobile replica, data validation, RBDV

I. INTRODUCTION

In Recent years, the largest developments of robotics have made it possible to develop a new environment for sensors to acquire the protection of sensor nodes from replication of it. The WSN contains group of nodes where each node is connected to one or more sensors and it could be used for a variety of applications including intruder detection, border monitoring and military patrols. Mobile replicas, basically small robots with sensing, wireless communications, and movement capabilities, these capabilities are useful for employing deployment of static sensor nodes, adaptive sampling, network repair and event detection [4]. In potentially hostile environments the security of unsupervised mobile node is highly vital.

The attacker can capture and compromise mobile nodes and use it to inject fake data, disrupt network operations and heeding the network communications. The replica node attack [11], dangerous attack in which the adversary takes the confidential data from a compromised node, generates a huge number of attacker-controlled replicas that share the compromised node’s keying materials and ID and spreads these replicas throughout the network. An adversary can create as many replica nodes from the single captured node. Replica nodes need not be identical robots, a group of mobile nodes can mimic the motion of a robot and other mobile nodes or even humans with hand-held devices can be used. Attacker has the software and keying material to communicate in the network, which can be obtained from the captured node entirely. An adversary controls the replica nodes but they allow the replica nodes which have keying materials to appear like authorized participant in the networks. Communications protocols for secure sensor network would allow replica nodes to produce pair wise shared keys with other nodes and the base station, thereby sanctioning the nodes to encrypt, decrypt, and authenticate all of their communications as though they were the original captured node. Several software based detections schemes were proposed to identify the replica nodes in static sensor nodes [3], [11], [17].The basic technique is that nodes identify the location and report it, if there is any contradictory reports that single one node in multiple locations. However, when the nodes are expected to move the fixed node location schemes not used.

The mobility-based replica detection schemes have been proposed based on the sequential probability Ratio test (SPRT) for mobile sensor networks [15]. Benign node never moves at speeds in excess of the system configured maximum speed because genial sensor node’s speed will almost be less than the system configured maximum speed. The speed measurement system is employed for the replica nodes are in two or more places at the same time in the network, this makes the replicated node is moving much faster than the benign nodes and thus replicated nodes measured speed is over the system configured maximum speed.

The Sequential Probability Ratio Test [15] which is a statistical decision process, it can be esteemed as one dimensional random walk with the lower and upper limits [8]. In which the null and alternate hypotheses are associated with the lower limit and an upper limit. The SPRT is well fitted for tackling the mobile replica detection problem, observed speed of mobile node is determined by the random walk with the two limits is constructed. The lower and upper limits can be configured to be associated with speeds should be less than and in excess of Vmax, respectively. Each time the mobile node’s speed exceeds (respectively, remains below) Vmax, it will hasten the random walk to hit or cross the upper (respectively, lower) limit and thus direct the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station determines that a mobile node has been replicated, it lifts the replica nodes from the network.

Every mobile node moves to a new location, it should submit time and location information to neighbouring nodes and it decides whether to forward the received claim to base station or not. Specifically, the main attack against the SPRT based scheme is encountered while replica nodes failed to render signed location and time information for speed measurement, when the nodes are ignoring minimum number of selective claim request from neighbouring nodes to avoid detection. Quarantine defence technique is employed to block the bulker nodes and the replica node attacks are stopped when many claims are ignored. First, the quarantine analysis technique is employed that the amount of time the replicas can affect the network is confined during one time slot but within single time slot does not fully reflect the interactions between attacker and defender. Second, game-theoretic analysis that shows the limits of any attacker strategy over many number of time slots. Two player repeated game model is formulated to model an interaction between the aggressor and the protector, to derive the optimal attack and defence strategies, it shows that the attacker's gain is greatly limited by the respective optimal strategies.

In the existing approaches the detection of replica node is purely based on the mobility of nodes. First, Sensor nodes are in mobility and mobile replicas are in static. Using the RSS (Received Signal strength) of received packet distance between sink and nodes are estimated, if the distance is remain constant than the node is determined as replica node. Second, using the speed variation of mobile nodes, the replica nodes are identified. However, where the sensor nodes and the mobile replica have the same mobility; it's difficult to find replicas in sensor networks. We propose a novel mobile replica detection scheme based on the reputation based data validation [19] in wireless sensor networks.

In the proposed scheme replica devices are identified using data validation, the data is forwarded to each node in wireless sensor networks along with the mobility of nodes. The data received from the nodes are periodically monitored; using directional antenna the angle of mobile nodes is estimated and using RSS (Received Signal Strength) of packet distance to sink is estimated. Using these information node position and neighbour can be identified and thus the complete network is partitioned into the sets. Data validation is applied to data received from these sets. Normally the sensed data from a single set is almost same in sensor network; in order to find the variation among these nodes the average data variation is estimated. The average value is calculated over the sensor nodes and the reputation values for mobile devices are periodically estimated by comparing the average value with the sensed data from sensor nodes. If the reputation value is greater than the predefined threshold then the node is determined as replica. Whenever the system decides that a node has been replicated based on a single observation of a node moving faster than it should get many false positives because of errors in speed measurement. False negative rates are occurred in high, when raising the speed threshold value. To minimize these false positives and false negatives, we apply the reputation based data validation method can make decisions quickly and accurately. We evaluate the performance of the proposed scheme via simulation study using ns-2 simulator. We validate the effectiveness, efficiency, and robustness of our scheme through the simulation experiments.

The rest of the paper is organized as follows: Section1 presents the related work. The problem statement, network assumptions and adversary models for the scheme is described in section3. Section4 presents the proposed mobile replica detection scheme using the reputation based data validation. Section 5 presents the simulation results of the proposed scheme. Finally, the paper is concluded in section 6.

II. RELATED WORK

Parno et al. [11] first proposed two schemes for the distributed detection of replica node attacks in sensor networks i.e. Randomized and Line selected multicast schemes. The two schemes are used to detect node location claims and identify their positions if there is any conflicting report that single one node is replicated in multiple locations. Conti et al. [3] and Ho et al. [6] proposed schemes to identify the replica nodes through the enhancement of line selected multicast scheme and group deployment knowledge to reduce storage overhead, communication and computation for the detection but the schemes [11], [3], [6] are not suitable for mobile sensor networks because of mobility of nodes the location will conflict with each other.

In the scheme [17], the fingerprint based detection mechanism for sensor nodes has a less storage overhead/ communication and high detection accuracy through checking the fingerprint for each sensor node enclosed in it and verifies the fingerprints by the detection probability of both base station and neighbouring sensors for each message it encounters. The real time detection of node attacks scheme [17] is used in mobile sensor network, movement of nodes makes conflicts in fingerprints of the same genial nodes.

Lately, Yu et al. [18] proposed a fresh efficient and distributed detection scheme for the replica node attacks in mobile sensor networks by the time interval calculated between the nodes encountered by mobile replicas more than of nodes encountered by benign nodes and it detects the replicas in the distributed manner.

Suat et al. [19] proposed a reputation based reliable data aggregation and transmission (RDAT) for the detection to prevent replica node attacks by using Reed- Solomon coding scheme based on multipath transmission algorithm improved the reliability of nodes but the scheme also has a good reliability in the presence of compromised node has a more storage overhead. Laura et al. [20] proposed a reputation based framework for sensor networks to provide the community of trust and data accuracy when the compromised nodes are present, the scheme used to detect the replicas and revoke the replicas compared to in [3], [6], [11], [17] used in mobile sensor networks.

III. PROBLEM STATEMENT

An opponent creates replica node u0 (it has the same ID and keying materials as mobile node u) from benign node, he first compromises and extracts possible secret keying materials from the genial node u, he can prepare a new node u0 and set the ID and secret keying materials of u0 alike u (u0, u1,…. un) then perhaps multiple compromised nodes and duplicated nodes in the sensor network. Our main goal is to detect the reality that both u and u0 operate as distinguished entities with the same identity and keys.

A. Network Assumptions

In the two-dimensional mobile sensor network, sensor nodes can freely roam into the network, every sensor node movement is physically limited by the predefined threshold value. Each node having capability to obtain location information from neighbour nodes to verifying the positions because the nodes communicated with the base station and other nodes through bidirectional links. The secure time synchronization protocols [12], [13] are used to synchronize the clocks of all nodes and secure localization methods [2], [7] are implemented by using the location information. The nodes communicate with the base station on a regular basis and base station may be static or mobile although we focus on a static base station for the simulations.

B. Attacker Models

We assume that an adversary may compromise and control the sensor nodes in the sensor networks, he can inject fictitious data packets into the network and interrupt local control protocols are localization, time synchronization, and route discovery process. Moreover, he can launch denial-of-service attacks by jamming the signals from genial nodes and we place some limits on the ability of the adversary to compromise nodes. The dangerous attacker model is replica node attack, he can produce many replica nodes and it will be accepted as a legitimate part of the network, within single captured node he can create as many replicas and allow them randomly move in the network. We assume the network operator collects and controls all sensor data operations by the base station because the base station is an entrusted entity, although the base station is compromised network when the sensor network is weakened completely before the mission starts.

IV. PROPOSED MODEL

This section provides the description about proposed scheme to detect replica node attacks in sensor networks. In wireless sensor networks have many subsisting and visualized applications for the ease of deployment especially in remote areas but the security of the WSN is an issue. To ensure the data authentication and integrity approaches are not sufficient for the misbehaviours encountered in WSNs. The use of reputation based data validation systems in wireless sensor network has become more prominent and an important mechanism to detect replica nodes based on data received from sensor nodes to the base station. In the existing approaches provides general reputation schemes to extenuate the effect of replica node attacks. The proposed scheme mainly implemented to detect the nodes ignoring the claim requests which are received from the neighbouring nodes to the base station so that an attacker may prepare the data as like defender such as location, time and data to be transmitted in the network, to prevent this data validation scheme is used effectively to find and revoke the nodes in the sensor networks.

In the proposed scheme replica devices are identified using data validation. In the data validation scheme, data received from the nodes are periodically monitored; using directional antenna angle of mobile nodes are estimated and using RSS (Received Signal Strength) of packet distance to sink is estimated. Using the information node position and neighbour can be identified using this information, so the disjoint set formation is performed that is complete network is partitioned into disjoint sets.

In data collection process, the data’s are collected from sets that are to be sensed by sensors. Data validation is applied to data received from these sets. The average value is calculated between the sensed data’s as follows:

$$\text{Average value} = \sum_{i=1}^{n} senseddata \qquad (4.1)$$

Where n = no of nodes in the sets.

Based on threshold value the Upper bound and Lower bound is calculated as:

Average value + Threshold value = UB (4.2)
Average value - Threshold value = LB (4.3)

Where UB= Upper Bound, LB= Lower Bound. Normally the sensed data from a single set is almost same in the sensor networks. In order to find the variation among these nodes the average data variation is estimated. By comparing the average value and sensed data from sensor nodes, reputation value for mobile devices are periodically estimated. If the reputation value is greater than the predefined threshold, the node is determined as replica then the reputation value for sensor node is incremented or decremented either when reputation value is less than (respectively, greater than) Lower Bound (respectively, Upper Bound). The detection of misbehaviours nodes along with the reputation system of WSN makes this model more efficient, robust and secure.

V. SIMULATION AND RESULTS

We simulated the proposed reputation based data validation for mobile replica detection scheme with the help of ns-2 simulator. The 500 mobile sensor nodes are positioned within the network topology area of 500 m x 500 m. We use the Two Ray Ground/ Random waypoint mobility (RWM) to evaluate the performance of the proposed scheme. In the data validation scheme, the node starts to send the data to neighbouring node i.e. data transmission interval is 0.1 sec. Based on pause time the node holds the data and send to another location of 20 milliseconds. The packet/ Data size may be vary from 500 Bytes to 2000 Bytes, in our simulation the packet size is 2000.

The transmission and receiving power of nodes that forwards/receives the data from neighbouring nodes to base station is 0.02 and 0.01 seconds. The data connections can occur randomly when the User Datagram Protocol (UDP) is used for the connection type and the Constant Bit rate (CBR) data traffic is used for the experimental results. The IDMRN protocol is used to analyse the proposed scheme in terms of false positive, detection delay, detection rate which is based on AODV routing protocol for the route discovery process.

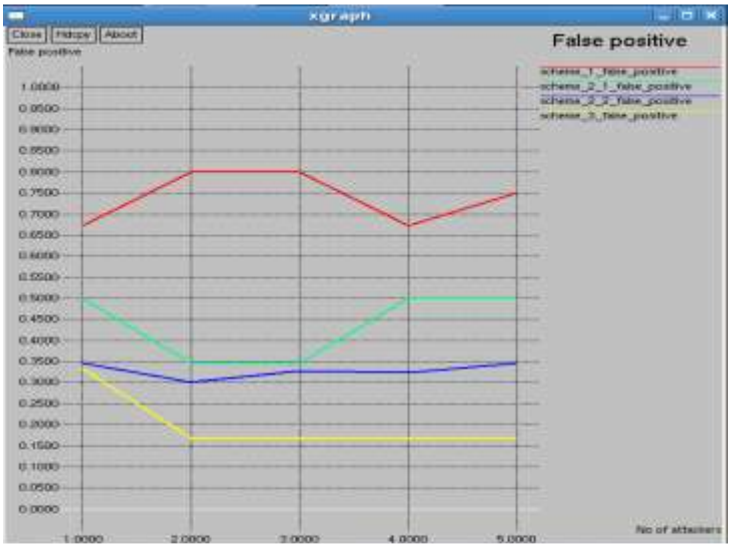

Fig.1 False positive rate

Each node uses the IEEE 802.11 (Wireless LAN) Medium Access protocol in which the transmission range is 30 m. To set the Upper Bound and Lower Bound for the proposed scheme is 1.0 and Omni directional antenna is used to find the direction of angle of mobile nodes, the node encounters 10.0 it will start sensing and the disjoint set is formed when node has a value as 5.0.

The performance of protocol is evaluated with respect to the number of attackers and number of nodes. Protocol performance is evaluated in terms of false positive, detection rate and detection delay. Compared to sequential hypothesis testing and defense strategy, the proposed system has a low false positive when the number of attacker increased. Fig .1 shows the false positive rate of nodes that are deployed into the network where the sensor node is known to be misidentified as a replica node is called false positive is to be minimized in the proposed system.

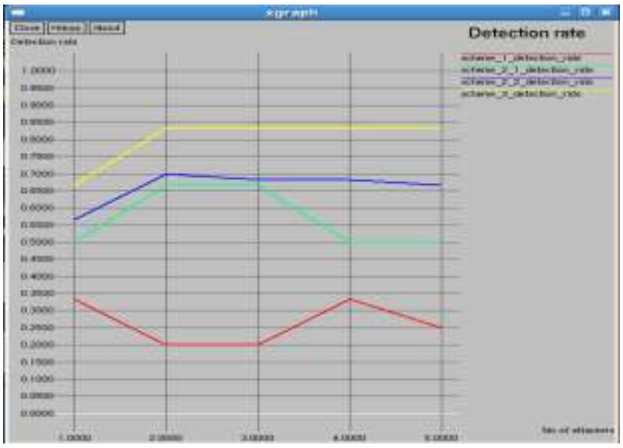

Fig.2 Detection rate

Fig.2 shows the protocol performance in terms of detection delay where the x and y axis indicates number of attackers and detection rate respectively. Reputation based data validation scheme achieves acceptable detection rate and it produces better performance compare to existing scheme in terms of detection rate. Fig .2 shows the detection rate is employed over the number of nodes that are deployed into the network where the maximum numbers of nodes are encountered as replica within the time interval is called detection rate and this comparison shows that the proposed method has the highest detection rate than the SPRT and defense strategies.

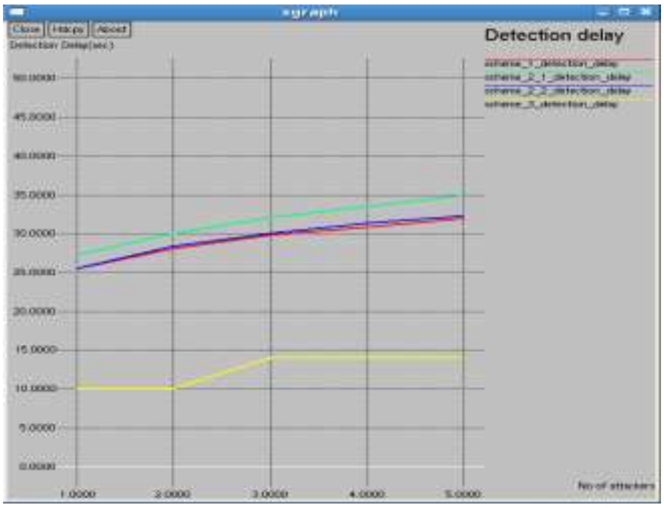

Fig .3 Detection delay

Protocol performance for the graph in Fig .3 shows the detection delay is measured across the number of nodes that are spread into the network and this comparison shows that proposed method has the minimum detection delay compared to the SPRT and quarantine defense analysis when the maximum number of attackers present in the network.

VI. CONCLUSION

This leads to protocol performance has the less detection overhead for the efficient, robust and secure mobile replica detection simulation results.

The replica detection scheme for mobile sensor networks based on SPRT was proposed to find replicas in wireless sensor networks. The quantitative analysis limits on the amount of time for which a group of replicas can avoid detection and quarantine. In game theoretic analysis, model the interaction between the detector and the adversary as a repeated game and found Nash equilibrium (NE). The proposed method reputation based data validation scheme is used to find replicas in the sensor networks when the nodes are ignoring the claim requests from the neighbouring nodes to base station. In order to find the nodes ignoring claims, the disjoint set estimation is employed therefore the sets are formed over the nodes of data to control the replicas. The results of the simulations show that proposed scheme quickly detects mobile replicas in wireless sensor networks in an efficient, secured and robust manner.

REFERENCES

[1]. J.Y.L.Boudec and M.Vojnovic "Perfect Simulation and Stationary of a Class of Mobility Models" Proc. IEEE INFOCOM, pp. 2743-2754, Mar. 2005.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

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

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

[9]. A.Liu and P.Ning "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks" Proc. Seventh IEEE Int'l Symp, Information Processing in Sensor Networks (IPSN), pp. 245-256, Apr. 2008.

[10]. S. PalChaudhuri, J.-Y.L. Boudec and M. Vojnovic "Perfect Simulations for Random Trip Mobility Models" Proc. 38th Ann. Simulation Symp, Apr. 2005.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. G. Theodorakopoulos and J.S. Baras "Game Theoretic Modelling of Malicious Users in Collaborative Networks" IEEE J. Selected Areas in Comm., vol. 26, no. 7, pp. 1317-1326, Sept. 2008.

[15]. Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajal K. Das "Fast Detection of Mobile Replica NodeAttacks in Wireless Sensor NetworksUsing Sequential Hypothesis Testing" IEEE Transactions on mobile computing, VOL. 10, NO. 6, JUNE 2011.

[16]. 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.

[17]. 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.

[18]. C.M.Yu, C.S.Lu and S.Y.Kuo "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks" Proc. IEEE Vehicular Technology Conf. Fall (VTC Fall), Sept. 2009.

[19]. SuatOzdemir "Functional reputation based reliable data aggregation and transmission for wireless sensor networks (RDAT)"Computer Communications (CS) 31 (2008) 3941–3953.

[20]. SaurabhGaneriwal, Laura K. Balzano, Mani B. Srivastava "Reputation-based framework for High IntegritySensor Networks" ACM Transactions on Sensor networks, Vol. V, No. N, September 2007.