International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 3, March 2014

Distributed and Fast Detection of Mobile Replica Node Capture Attacks Using Sequential Hypothesis Testing For WSN

Feba S Babu

Lecturer, Department of Electronics and Communication, College of Engineering, Kottarakara, Kerala, India

Abstract: ***Security is important for many sensor network applications. Wireless Sensor Networks (WSN) are often deployed in hostile environments as static or mobile, where an adversary collects all the credentials like keys and identity. The attacker can reprogram it and replicate the node in order to eavesdrop the transmitted messages or compromise the functionality of the network. A harmful attack against sensor networks where one or more nodes illegitimately claims an identity as replicas is known as the node replication attack. This paper detects the node replication attack using Efficient Distributed Detection, Scheme and Game theoretic approach to improve the performance***

Keywords: Replica detection, sequential analysis, efficient distributed detection scheme

1. Introduction

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Sensor nodes operate in hostile environments such as battle fields and surveillance zones. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. The mission-critical nature of sensor network applications implies that any compromise or loss of sensory resource due to a malicious attack launched by the adversary-class can cause significant damage to the entire network. Sensor nodes deployed in a battlefield may have intelligent adversaries operating in their surroundings, intending to subvert damage or hijack messages exchanged in the network. The compromise of a sensor node can lead to greater damage to the network. The resource challenged nature of environments of operation of sensor nodes largely differentiates them from other networks. All security solutions proposed for sensor networks need to operate with minimal energy usage, whilst securing the network. So the basic security requirements of WSN are availability, confidentiality, integrity and communication.

Sensor network attacks are classified into three main categories: Identity Attacks, Routing Attacks & Network Intrusion. Identity attacks intend to steal the identities of legitimate nodes operating in the sensor network. The identity attacks are Sybil attack and Clone (Replication) attack. In a Sybil attack, the WSN is subverted by a malicious node which forges a large number of fake identities in order to disrupt the network's protocols. A node replication attack is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network.

Routing attack intend to place the Rogue nodes on a routing path from a source to the base station may attempt to tamper with or discard legitimate data packets. Some of the routing attacks are Sinkhole Attack, False routing information attack, Selective forwarding attack, and False routing information attack, Selective forwarding attack, and False routing information attack, Selective forwarding attack, and Wormholes. The adversary creates a large sphere of influence, which will attract all traffic destined for the base station from nodes which may be several hops away from the compromised node which is known as sinkhole attack. False routing attack means that injecting fake routing control packets into the network. Compromised node may refuse to forward or forward selective packets called as selective forwarding attack. In the wormhole attack two or more malicious colluding nodes create higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points.

The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. Several software-based replica node detection schemes have been proposed for static sensor networks. The primary method used by these schemes is to have nodes report location claims that identify their positions and for other nodes to attempt to detect conflicting reports that signal one node in multiple locations. However, since this approach requires fixed node locations, it cannot be used when nodes are expected to move. Thus, the challenge is to design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks.

In the existing work a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT) is proposed. SPRT is a centralized distribution scheme. In the proposed system an efficient distributed detection system with game theoretic approach is implemented.

2. Related Work

The first work on detecting replica node attacks is due to Parno et al. [3], who proposed randomized and line-selected multicast schemes to detect replicas in static wireless sensor networks. In those two schemes, nodes report location claims

that identify their positions and attempt to detect conflicting reports that signal one node in multiple locations.

Conti et al. [4] proposed a scheme to enhance the line-selected multicast scheme of [3] in terms of replica detection probability, as well as storage and computation overheads by using trusted random values. Ho et al. [2] proposed several schemes for distributed detection of replica nodes that take advantage of group deployment knowledge to reduce the communication, computation, and storage overheads required for replica detection and improve on the replica detection capability of the line-selected scheme of [3].

Xing et al. [5] proposed a fingerprint-based replica node detection scheme. In this scheme, nodes report fingerprints, which identify a set of their neighbors, to the base station. The base station performs replica detection by using the property that fingerprints of replicas conflict each other. However, none of these solutions is suitable for replica node detection in mobile sensor networks. If the schemes in [4], [2], [3] are used in mobile sensor networks, sensor nodes' location claims will be continuously changed in accordance with their movements, and thus location claims from the same benign node will always conflict each other. Similarly, if the scheme in [5] is used in mobile sensor networks, mobility will continuously make nodes have different fingerprints, and thus fingerprints of the same benign node will conflict each other.

Recently, Yu et al. [18] proposed schemes to detect node replica attacks in mobile sensor networks. The key idea of [18] is to detect mobile replicas by leveraging the intuition that the number of mobile nodes encountered by mobile replicas in a time interval is more than the number encountered by a benign mobile node.

Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajal K. Das, Senior Member, IEEE, proposed a centralized detection scheme based on sequential hypothesis testing. In this Sequential Probability Ratio Test (SPRT) along with Game theoretic approach is used to detect the replica node capture attacks. The fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed as long as a speed measurement system with a low error rate is employed. On the other hand, replica nodes are in two or more places at the same time. This makes it appear as 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 the 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. However, if the system decides that a node has been replicated based on a single observation of a node moving faster than it should, many false positives are obtained because of errors in speed measurement. 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, apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately. The SPRT is performed 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 nodes will be revoked from the network. SPRT proceeds in two phases:

2.1 Claim Generation and Forwarding

Each time a mobile sensor node u moves to a new location, it first discovers its location Lu and then discovers its set of neighboring nodes, N(u). Every neighboring node v Є N(u) asks node u for an authenticated location claim by sending its current time T to node u. Upon receiving T, node *u* checks whether T is valid or not. If $|T'-T|>\delta+\varepsilon$, where T' is the claim receipt time at *u*, δ is the estimated transmission delay of claim, and ε is a maximum error in time synchronization, then node *u* will ignore the request. Otherwise, *u* generates location claim $C_u=\{u||L_u||T||Sig_u\}$ sends it to v, where Sig_u is the signature of the tuple (u, L_u, T) generated using node u's private key. If u denies the claim requests, or if its claim contains invalid time information or fails to authenticate, then u will be removed from N(v). Also, if u claims a location Lu such that the distance between Lv and Lu is larger than the assumed signal range of v, then it will be removed from N(v). Once the above filtering process is passed, each neighbor v of node u forwards u's claim to the base station with probability p.

2.2 Detection and Revocation

If a mobile node u is judged as benign, the base station restarts the SPRT with newly arrived claims from u. If, however, u is determined to be replicated, the base station terminates the SPRT on u and revokes all nodes with identity u from the network.

SPRT is a centralized distribution scheme. So another method is proposed, which is called Efficient and Distributed Detection scheme. In the proposed work, EDD is combined with game theoretic approach to improve the performance.

3. Proposed Work

To detect the node replicas in mobile sensor networks, an Efficient and Distributed Detection (EDD) scheme is used. EDD possess the following characteristics. 1) Distributed Detection: EDD can resist against the node replication attacks in a distributed fashion without involving the base station. 2) Individual Detection: Each node in the EDD scheme is able to detect replicas by itself. 3) Network-Wide Revocation Avoidance: The revocation of the replicas can be performed by each node without flooding the revocation messages to the entire network. 4) Efficiency and Effectiveness: The EDD scheme can identify the replicas

with high detection accuracy. In the proposed work centralized detection scheme called SPRT is compared with the EDD. To improve the performance EDD is combined with the Game theoretic approach.

4. Block Diagram

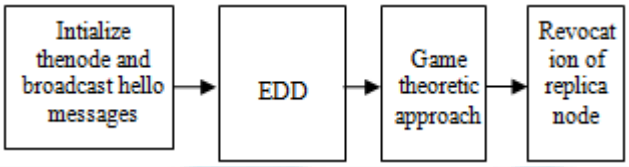

Figure 1: block diagram

The idea behind EDD is motivated from the following observations. For a network without replicas, the number of times, $\mu 1$, that the node u encounters a specific node v, should be limited in a given time interval of length T with high probability. For a network with two replicas v, the number of times, $\mu 2$, that u encounters the replicas with the same ID *v*, should be larger than a threshold within the time interval of length T. According to these observations, if each node can discriminate between these two cases, each node has the ability to identify the replicas.

The EDD scheme is composed of two steps: off-line step and on-line step. The off-line step is performed by the network planner before the sensor deployment. The goal is to calculate the parameters, including the length T of the time interval and the threshold ψ used for discrimination between the genuine nodes and the replicas. On the other hand, the on-line step will be performed by each node per move. Each node checks whether the encountered nodes are replicas by comparing ψ with the number of encounters at the end of a time interval.

For fault free revocation EDD is combined with the game theoretic analysis. In this a two player repeated game with perfect information is formulated where the two players are the attacker and the defender. In the proposed work this G-EDD is compared with the SPRT analysis. *Security and Performance Evaluation:*

Detection Time: When the replicas are placed into the network at a certain time interval T_i, they can be detected at the time interval T_{i+1} with high probability. In other words, if the replicas exist, at most 2T time units are required to finish detection. In case the replicas utilize the selective silence, only one genuine node finding such replicas can flood the revocation message to the network. Thus, the replicas adopting selective silence will be revoked almost immediately.

Storage Overhead: The storage overhead for the EDD scheme is O(n). It appears that EDD is inapplicable to the sensor networks. However, EDD is found to be applicable for current mobile sensor networks according to the following observations: 1) Compared with the inherent characteristics of sensor nodes such as limited communication capability and battery power, the limited storage can be properly relaxed by either attaching memory module to the sensor node or exploiting advanced sensor nodes. 2) The current sensor networks usually consist of tens of sensor nodes. In other words, the scale is not large and each element in the list L only needs several bits in practice so that the storage overhead O(n) is affordable for the current sensor nodes. If the sensor nodes with extremely scarce resource are considered or the scale of the network is relatively large, then the EDD scheme might be inapplicable for the sensor nodes.

Computation Overhead: The off-line step of EDD may be a time-consuming task. However, it is executed, prior to the sensor deployment, by the network planner instead of the sensor node. In addition, since the network planner usually at least has PC-level computation power, this task can be successfully accomplished. As to the computation overhead of sensor nodes, in addition to the operations required for the signed messages, only simple arithmetic operations such as addition and set operations such as intersection are required to be performed, which are affordable for the current generation sensor nodes.

Communication Overhead: It is known that communication dominates the energy consumption of a sensor node. Hence, to reduce the energy consumption of networks, it should emphasis on reducing communication overhead. In the EDD schemes, each node u listens the beacon $b_{v,i}$ =(v, ω_v ,ti) broadcasted by its neighbor v. Upon receiving the beacon, the node u checks if v is a replica by executing the on-line step of EDD. It can be observed that the additional communication overhead incurred by the EDD scheme is only b_v, resulting in O(1) communication overhead in general case. Even better, when certain applications such as tracking are considered, since the periodical broadcast of beacon has been required in such an application, the communication overhead could become zero by piggy-backing $\omega_{v,i}$ the broadcasted message. One special case is the network with replicas adopting selective silence, which can be discovered and revoked by flooding revocation messages with O(n) communication overhead.

5. Simulation Results

The metric used to evaluate the performance of the schemes are:

- *Number of claims:* is the number of claims required for the base station to decide whether a node has been replicated or not.
- *True positive:* is the probability that a replica node is identified as a replica node.
- *True negative:* is the probability that a benign node is identified as a benign node.
- *False positive:* is the error probability that a benign node is misidentified as a replica node.
- *False negative:* is the error probability that a replica node is misidentified as a benign node.

The results of the average number of claims are shown below. One is that the claim generator is a benign node and the SPRT decides that this node is benign. This case is denoted by true Negative in below Fig. The other case is that the claim generators consist of a compromised node and its

replica node, and the SPRT decides that these nodes are compromised node and its replica. This case is denoted by true Positive in below Fig.

In the true Negative case, the average number of claims reaches a maximum of 5.03 when Vmax =80 m/s and γ=0.1. In the true Positive case, the average number of claims reaches a maximum of 9.089 when Vmax = 10 m/s and γ= 0.1 Thus, the base station reaches correct decisions with a few claims in both cases.

Observed that the average number of claims tends to slightly increase and decrease as mobility rate rises in the case of true Negative and true Positive, respectively. From this observation inferred that a rise in mobility increases the chance that the speed of a benign node is erroneously measured to be over Vmax, thus delaying the test from moving toward H0. On the other hand, a rise in mobility leads to a reduction in the chance that the replicated node generates claims containing the same location but different time, and thus expedites moving the test toward H1.

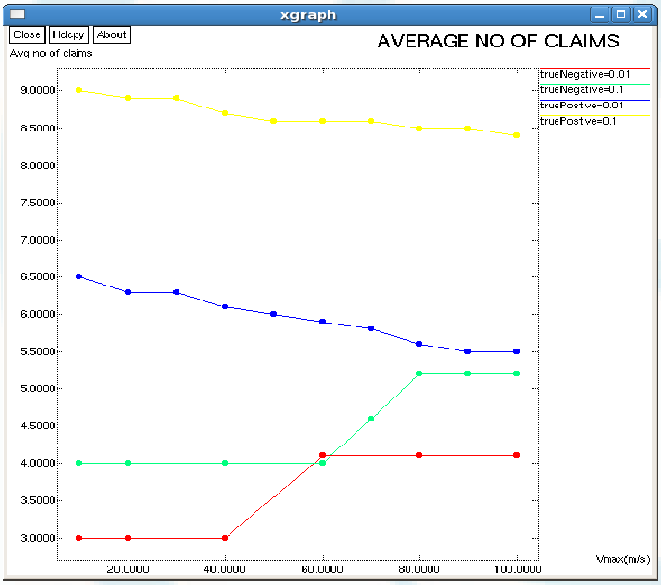

Figure 2: Average number of claims versus Vmax

The results of the average number of claims versus D(m), when Vmax=40m/s is shown below.

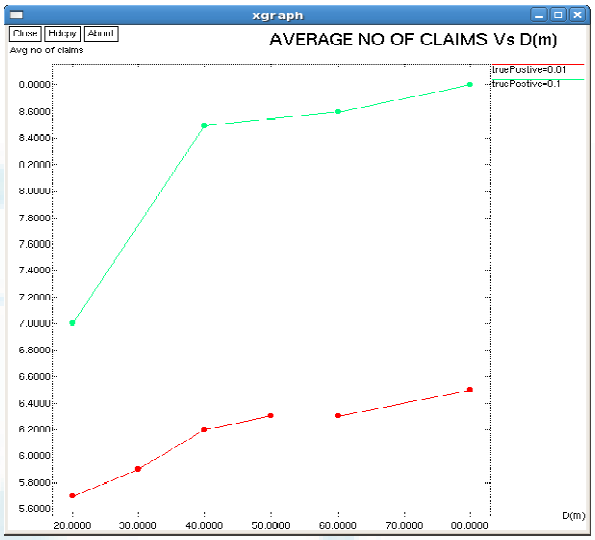

Figure 3: Average number of claims versus D(m),when Vmax=40m/s

The results of the packet lost due to replica node and using SPRT without replica node is shown below.

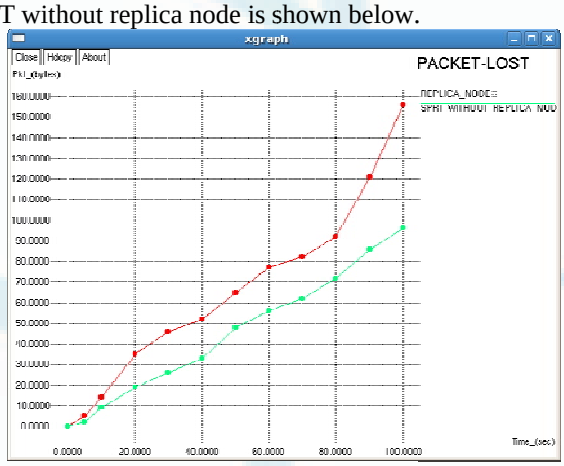

Figure 4: Packet lost versus time

The result of the packet lost due to SPRT is compared with the EDD is shown below.

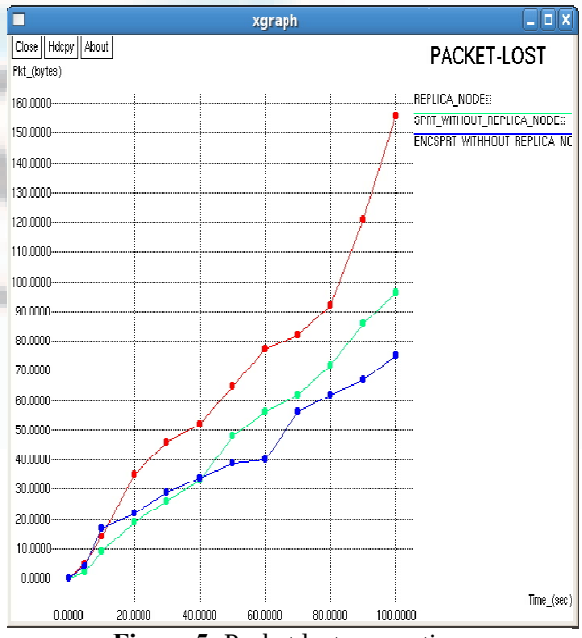

Figure 5: Packet lost versus time

6. Conclusion

In this paper a centralized detection scheme called SPRT is implemented. And a distributed detection scheme which is Efficient Distributed Detection Scheme along with game theoretic approach is implemented. This G-EDD improves the revocation mechanism and it is effective and efficient in terms of the communication/computation/storage overheads. Then it is compared with the SPRT analysis to study the relation between SPRT and EDD.

References

[1] Jun-Won Ho, Matthew Wright, Senior Member, IEEE" Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing," vol. 10, no. 6, June 2011.
[2] 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.
[3] 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.
[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. 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.
[6] 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.
[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] 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.