Energy Efficient Finite Range Query Scheme for Detecting Mobile Adversary Replica Nodes in Wireless Sensor Networks

S.Kumaravel
Research Scholar, Manav Bharti University, Solan (Hp)

ABSTRACT

With the growing demand in wireless sensor network (WSN), adversary attack on sensor node becomes major issue in current WSN deployment. The replica nodes which are generated by attackers receive the valuable information from the network in turn sends to the adversaries and at the same time transmits inappropriate message to the sink in the sensor networks. One of the existing works presented Sequential Probability Ratio Test (SPRT) which reduces the overhead of sensor node transmission on the adversary conditions. However, the sensor node's mobility affected the query range being invoked for detection of replica node location with probability ratio. The energy efficiency of the sensor node also needs to be monitored for effective adversary sensor node detection using SPRT.

Our proposed work extends replica detection scheme of probability ratio test with Finite Range Query (FRQ) technique to effectively identify the mobile replica nodes (acting as adversary) and eliminate the varying query ranges of mobile sensor nodes. In addition energy efficiency of the sensor nodes are improved by minimizing the message query transmission on data aggregation.

1. INTRODUCTION

A latest set of security confronts grows in WSN because of the fact in which present sensor nodes require hardware maintain for tamper-resistance and are frequently arranged in unattended environments which are susceptible to confine and compromise by an adversary. A severe outcome of node compromise is which an adversary has acquired the qualifications of a sensor node, it can secretly place in replicas of that node at planned locations inside the network. These replicas will be used to initiate a variety of insidious and tough to find the attacks on the sensor application and the fundamental networking protocols. The mobile replica node is a node which having the similar ID and secret keying materials as a mobile node. An adversary generates replica node by compromises the original mobile node and discovers all secret keying materials from it. Then organizes a new node, sets the ID of original mobile node, and original node's secret keying materials are loaded. There will be multiple replicas of the original node and multiple compromised and replicated nodes. The objective is to notice the fact that both innovative and replicated nodes as divide entities with the similar identity and keys.

Each mobile sensor node is able of getting its location information and also validating the locations of its neighboring nodes. This can be executed by employing secure localization methods in which clocks of all nodes are loosely coordinated. This can be achieved with the help of safe time synchronization protocols. The nodes in the mobile sensor network communicate with a base station. The base station might be static or mobile, although we focus on a static base station for our simulations, as long as the nodes contain a way to converse reliably to the base station on a usual basis. An adversary will compromise and completely manage a subset of the sensor nodes, permitting him to mount different types of attacks similar to DDOS attacks by jamming the signals from benevolent nodes.

To increase his efficiency, the adversary also initiates a replica node attack, which is the focus of our research. The adversary produces many replica nodes and that they will be conventional as a legal part of the network. The attacker tries to spend as many replicas of one or more compromised sensor nodes in the network as will be efficient for his attacks. The attacker permits his replica nodes to randomly travel or he shifts his replica nodes in dissimilar patterns in an effort to frustrate our Energy Efficient Finite Range Query Scheme.

In this paper, the proposal work extends replica detection scheme of probability ratio test with Finite Range Query (FRQ) technique. This technique discovers the mobile replica nodes which is acting as an adversary and remove the query range variations of mobile sensor nodes and also the proposed technique improves energy efficiency of the sensor nodes by reducing the message query transmission on data aggregation.

2. LITERATURE REVIEW

Several schemes were provided for distributed detection of replica nodes that take advantage of group deployment knowledge to reduce the communication, computation, and storage overheads. It is highly required for replica detection and improved on the replica detection capability of the line-selected scheme [1]. In Fingerprint-based replica node detection scheme [2], nodes report fingerprints, which identify a set of their neighbors, to the base station [8]. The base station performs replica detection by using the property that fingerprints of replicas conflict each other [4]. However, none of these solutions is suitable for replica node detection in mobile sensor networks. Another scheme in [3] is 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 [5].

Similarly, if the scheme in [6] is used in mobile sensor networks, mobility will continuously make nodes with different fingerprints [7], and thus fingerprints of the same benign node will conflict each other. Recently, Yu et al. [9] proposed schemes to detect node replica attacks in mobile sensor networks. The key idea of [10] 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 [11].

Therefore, our scheme works with less overhead than those in [12]. The main strength of [13] is that it detects mobile replicas in fully distributed manner, while our scheme extends mobile replica detection to remove the query range variation. However, replicas can evade this detection technique by carefully controlling the number of encounters each replica has with other nodes. The attacker can selectively use its encounters to maximize the effectiveness of the attacks it is trying to mount with the replica nodes. Since this puts a limitation on the attacker, it remains to be studied whether the detection scheme is enough to deter effective replica attacks

3. ENERGY EFFICIENT FINITE RANGE QUERY SCHEME TO DETECT MOBILE ADVERSARY REPLICA NODES IN WSN

Our proposed technique, the replica detection scheme of probability ratio test with Finite Range Query (FRQ) is to detect replica node attacks in mobile sensor networks. In static sensor networks, a sensor node is observed as being replicated if it is located in more than one position. If nodes are moving around in network, though, this technique does not work, because a benevolent mobile node will be treated as a replica because of its incessant change in location. Therefore, we should use some other method to identify replica nodes in mobile sensor networks. Providentially, mobility offers us with a evidence to assist resolve the mobile replica discovery problem. We propose a mobile replica detection scheme by leveraging this intuition.

Proposed Energy Efficient Finite Range Query Scheme (fig 1) is well matched for attempting the mobile replica detection problem while we build a random walk with two limits in such a way that every walk is determined by the experimented speed of a mobile node. The lower and upper limits will be configured to be connected with speeds less than and in overload of Vmax, correspondingly. We relate the Energy Efficient Finite Range Query Scheme to the mobile replica detection crisis as follows. Every time a mobile sensor node travels to a novel location, every one of its neighbors requests for a marked claim having its location and time information and determines probabilistically whether to forward the received claim to the base station. The base station calculates the speed from all two successive claims of a mobile node and achieves the Energy Efficient Finite Range Query Scheme by allowing for speed as an observed model. Every time the mobile node's speed beats (respectively, remains below) Vmax, it should accelerate the random walk to hit or cross the upper (respectively, lower) limit and therefore guide to the base station accepting the exchange (respectively, null) suggestion in which the mobile node has been (respectively, not been) replicated. Once the base station makes a decision that a mobile node has been replicated, it eliminates the replica nodes from the network.

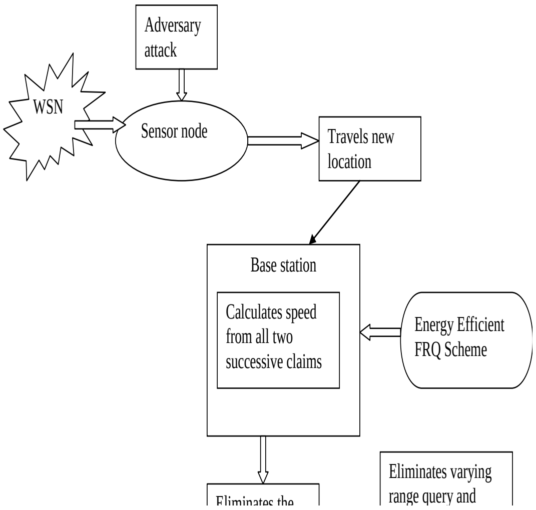
Adversary attack
WSN
Sensor node
Travels new location
Base station
Calculates speed from all two successive claims
Energy Efficient FRQ Scheme
Eliminates the
Eliminates varying range query and

Fig 1. Energy Efficient FRQ scheme

3.1. SECURITY ANALYSIS

The metrics used to evaluate the security of the SDC scheme are: 1) the probability of detecting node replication when adversaries put x replicas (including the compromised node) with the same identity into the network, which is denoted as pdr; 2) the probability that adversaries control all the witnesses for a given identity after compromising t nodes, which is denoted as pts.

3.2 DETECTING REPLICAS

The nodes storing the copies of a location claim are chosen randomly from the whole network, such nodes are chosen randomly from a small subset of all the nodes in the network. Let Es1 denote the set of all the combinations of choosing 1 to *v*−1 elements from E, i.e., the set to which IDL is mapped. If the node replication attack is not detected when the adversary adds replica r2 to the network, this implies that the location claims for r2 were forwarded to a set of nodes that do not have any nodes that store the previous location claims of r1. Let Ee1 denote a subset of the nodes in E that do not store the location claims of r1. Let pm, 1 denote the probability that the location claim of r1 is forwarded to all the cells in E except the cells in Ee1, which is an element of Es1. Let pm, 2 denote the probability that the location claim of r2 is forwarded to any cell(s) in Ee1. Therefore, we have:

$$P2R = \sum_{m=1}^{|Es1|} pm1 * pm2 \quad \text{-------->}\ (1)$$

Let R = 3 and v = 3. According to Equation (1) FRQ scheme can achieve a very high replica detection rate

Now, we consider one step further the case that the adversary adds r3 to the network. Let Es1b denote the set of all the combinations of choosing 2 to v − 1 elements from E. For a given Ee1 ∈ Es1b, let Es2 denote all the combinations of choosing 1 to |Ee1| − 1 elements from Ee1. We denote Ee2 as the set of cells that store the location claim from r2 but not r1, and Ee2 ∈ Es2. Let pm denote the probability that the location claim of r1 is forwarded to all the cells in E except the cells in Ee1, which is an element of Es1b. Let pmn, 1 denote the probability that the location claim of r2 is forwarded only to all the cells in Ee2. Let pmn,2 denote the probability that the location claim of r3 is forwarded to any cell(s) in Ee1 except those in Ee2. Thus, we have:

$$P3R \; = \sum_{m=1}^{|Es1b|} \sum_{n=1}^{|Es2|} pm * pmn1 * pmn2 \quad \text{-->}\ (2)$$

As a result, compared to the SPRT approach, the success rate that adversaries control all the witnesses of a given identity is reduced in our proposed Energy Efficient FRQ Scheme.

4. PERFORMANCE ON ENERGY EFFICIENT FRQ SCHEME

We simulated the proposed mobile replica detection scheme in a mobile sensor network with the help of the ns-2 network simulator. In our simulations, we deploy n nodes uniformly at random within a 500 × 500 square, with n varying between 100 and 1000. We use the Random Waypoint Mobility (RWM) model to determine mobile sensor node movement patterns. In particular, to accurately evaluate the performance of the scheme, we use the RWM model with the steady-state distribution provided by the Random Trip Mobility (RTM) model. In the RWM model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed.

We assume the standard unit disc bidirectional communication model and we adjust the communication range, so that each node will have approximately 40 neighbors on average. We use an average of the total number of messages sent or received per node as a measure of the communication requirements, and we measure resiliency by counting the number of times we must run the protocol in order to detect a single node replication (i.e., we select a random node and insert one replica into the network).

After reaching that location, it stays there for a predefined pause time. After the pause time, it then randomly chooses and moves to another location. This random movement process is repeated throughout the simulation period. We use code from to generate RWM-based movement model with a steady-state distribution. All simulations were performed for 1,000 simulation seconds. We fixed a pause time of 20 simulation seconds and a minimum moving speed of 1.0 m/s of each node. Each node uses IEEE 802.11 as the medium access control protocol in which the transmission range is 50 m. To emulate the speed errors caused by the inaccuracy of time synchronization and localization protocols, we modify the measured speeds with maximum speed error rate.

5. RESULTS AND DISCUSSION

Our proposed Energy Efficient Finite Range Query Scheme is evaluated by using the following metrics.

i. Energy Efficiency
ii. Finite Range Query
iii. Adversary Replica Nodes

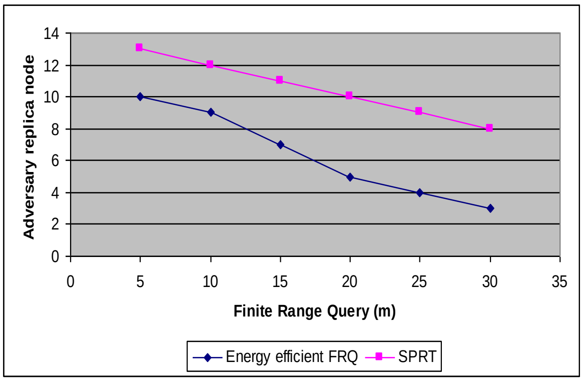

Fig 2: Finite range Query vs Adversary Replica node

In Figure 2, we compare the Energy efficient FRQ scheme with the SPRT scheme. As shown in Figure 3, in both the schemes, FRQ has the lowest has the lowest mobile replica node. As the finite query range increases, FRQ and SPRT have lower adversary replica node. Compared with SPRT, proposed FRQ scheme having the mobile replica node is relatively low.

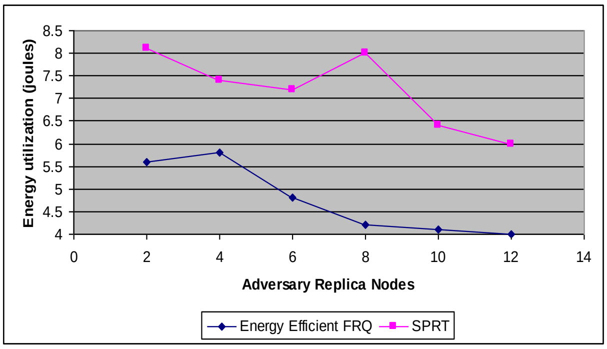

Fig 3: Adversary Replica node vs Energy utilization

In experiment, the number of adversary replica nodes is varied from 2 to 12 (Figure 3). The energy consumption of FRQ decreases dramatically when the replica nodes increases. This is because all queries are sent to the consolidator node to be stored. Our FRQ scheme consistently consumes less energy compared to SPRT.

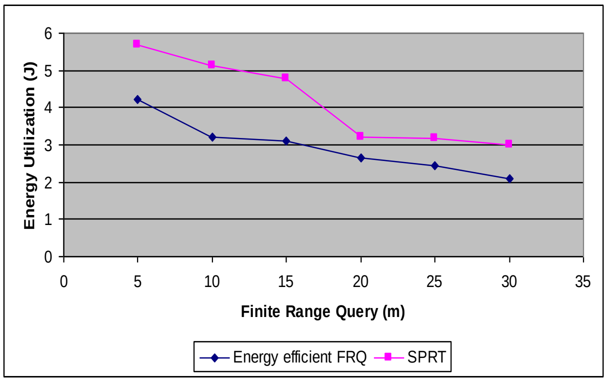

Fig 4: Finite range Query vs Energy utilization

In Figure 4, the number of Finite query varies from 5 to 30. The increase of Finite Query Range under leads to decrease the energy utilization in both the two schemes. Compared with existing SPRT energy efficient FRQ performs well.

6. CONCLUSION

The proposal work presented Energy Efficient Finite Range Query Scheme for Detecting Mobile Adversary Replica Nodes in Wireless Sensor Networks in which it extends replica detection scheme of probability ratio test with FRQ technique to finding the mobile replica nodes and removes the changing query ranges of mobile sensor nodes. This technique minimizing the message query transmission on data aggregation. We performed simulations of the scheme 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 from moving to best evade detection. The results of these simulations show that our scheme quickly detects mobile replicas with a small number of location claims against either strategy.

7. REFERENCES

[1] J. Ho, M. Wright, and S. K. Das, “Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 6, JUNE 2011.

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter. Detection of denial-of-message attacks on sensor network broadcasts. In Proceedings of IEEE Symposium on Security and Privacy, May 2005.

[11] 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 Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews, vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

[12] 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.” ACM MobiHoc, 2007.

[13] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, “Efficient Distributed Detection of Node Replication Attacks in Sensor Networks,” ACSAC, 2007.