Energy Efficient Detection of Replica Node in Mobile Sensor Networks

D.Vinoth Kannan
Department of Electronics and Communication Engineering
Kalasalingam University
Krishnankoil- india.

S.Bala Murugan
Department of Electronics and Communication Engineering
Kalasalingam University
Krishnankoil- india.

ABSTRACT

In Mobile Sensor Network, attacker can easily capture a node and compromise that sensor node and extract keying materials from that compromised node and make replicas of them. These replica node attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network .Then attacker use the replica node to inject fake data and disrupt the entire operations in the network. These Replica nodes are detected using System configure speed and neighbor identity method.

Keyword ---- Mobile node replication attack, Mobile Sensor node deployment, security.

1. INTRODUCTION

Wireless sensor network is a collection of sensor nodes with limited energy, memory and processing capabilities [1]. Due to the nature of deployment they are unattended. So an adversary can capture a sensor node easily and compromise it to get the keying materials and the program inside the node[2]. Providing security to an unattended node is a critical one. The most hazardous attack in this scenario is a node replication attack. By capturing a single sensor node, the adversary can create as many replicas as he has the hardware. Time taken for placing the replicas should be less than the time and effort taken for capturing and compromising the nodes.

A WSN can be deployed in harsh environments to fulfill both military and civil applications [3]. For instance, an adversary could eavesdrop on all network communications and could capture nodes thereby acquiring all the information stored within. Once a sensor is compromised, the information inside is easily accessible. An adversary may replicate captured sensors and deploy them in the network to launch a variety of insider attacks. This attack process is referred to as *clone attack[6]*.

The replica nodes are placed again in the network for more malicious activities. Finding a replica and recover from the replica node attack in the network is an essential one for providing security to the sensor nodes[4,5,7]. Detection of a replica node is not so easy since they have the legitimate keys which make them to consider as legitimate member of the network. After compromising a sensor node, an adversary can perform various attacks on the network in many ways. He can simply listening the traffic flow to gather information that passes through the nodes. He can perform jamming attack so that the legitimate signals cannot be transmitted. Alternatively he can inject some false information to corrupt the sensor node's operation or he can change the various network protocols for formation of clusters and then disabling the functions of the network.

A straightforward solution to stop replica node attacks is to prevent the adversary from extracting secret key materials from mobile nodes by equipping them with tamper-resistant hardware[8]. Although the tamper-resistant hardware can make it significantly harder and more time-consuming to extract keying materials from the captured nodes.

In this paper, a novel mobile replica detection scheme is proposed. An uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. On the other hand, replica nodes are in two or more places at the same time. So the replicated node move much faster than any of the uncompromised nodes, the system finds the replica node and rejects the replica node.

2. PRELIMINARIES

In this section, We first state the problem statement and network assumptions and describe the attacker models.

1) Problem Statement: In this, a mobile replica node is having the same ID and secret keying materials and denoted as u' .Mobile node is denoted as u. An attacker first compromise the mobile node u and extract the secret keying materials from the mobile node u, then he prepares a new replica node u' and set the same secret keying materials and same ID for u' as in u. So there may be multiple replicas of u.

2) Network Assumptions: Consider a two-dimensional mobile sensor network where the sensor nodes freely roam throughout the network. We assume that every sensor node in a network is limited by the system-configured speed, $V_{\max}$ .Also assume that all direct communication between sensor nodes is bidirectional. Assume that every mobile sensor node is capable of obtaining its location information and also verifying the locations of its neighbouring nodes. We also assume that nodes in mobile sensor network communicate with a base station.

3) Attackers Models: An attacker may compromise a mobile node and fully control all the sensor node in a network ,and inject the false data in to the network and disrupt the entire network operations.

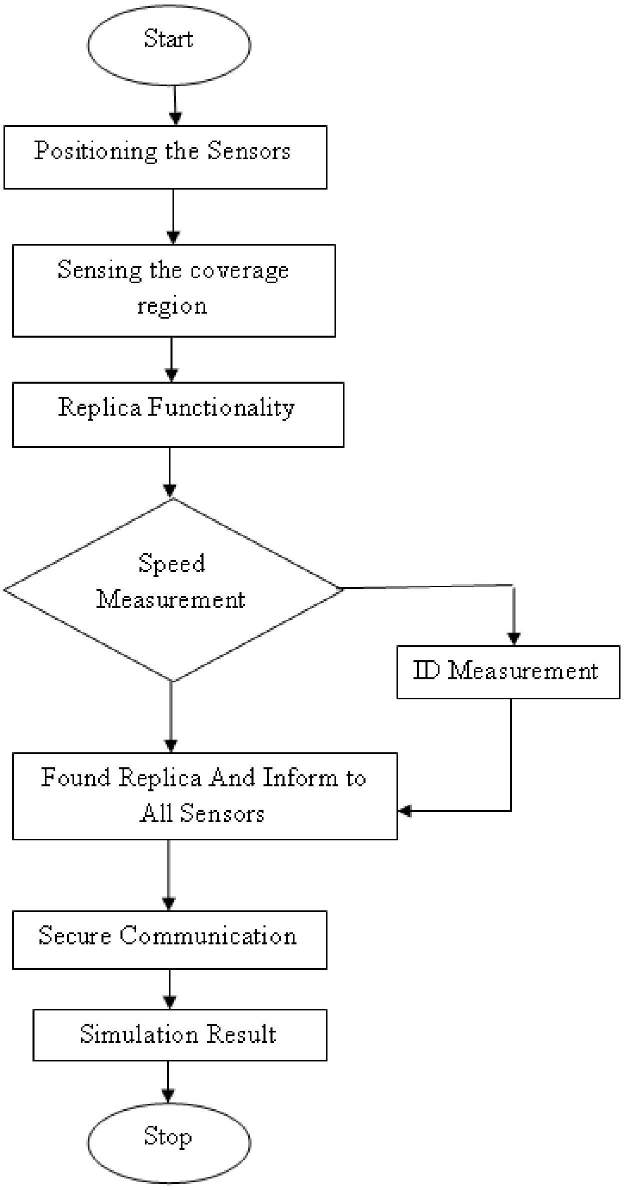
4) Design goals: First the replica node should be detected with reasonable communication, computational and storage overheads. Second the detection of replica node in a network should be robust.

3. MOBILE REPLICATION DETECTION

In static sensor networks, a sensor node is regarded as being replicated if it is placed in more than one location. If nodes are moving around in network, however, this technique does not work, because a benign mobile node would be treated as a replica due to its continuous change in location. Hence, we must use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem. Specifically, a benign mobile sensor node should never move faster than the system configured maximum speed, V max. As a result, a benign mobile sensor node's measured speed will appear to be at most V max as long as we employ a speed measurement system with a low rate of error. On the other hand, replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over V max because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds V max, it is then highly likely that at least two nodes with the same identity are present in the network.

We apply the neighbor identity to the mobile replica detection problem as follows: Each time a mobile sensor node moves to a new location, each of its neighbors asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the neighbor identity by considering speed as an observed sample. Each time the mobile node's speed exceeds (respectively, remains below) V max, it will expedite the random walk to hit or cross the upper (respectively, lower) limit and thus lead to the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network.

FLOW CHART-1



4. SIMULATION STUDY

1) Simulation Environment: We simulated the proposed mobile replica detection scheme in a mobile sensor network with the help of the ns-2 network simulator. In our simulation, 50 mobile sensor nodes are placed within a square area of 50 m _ 50 m.

The Random Waypoint Mobility (RWM) model is used to

determine mobile sensor node movement patterns. In particular, to accurately evaluate the performance of the scheme, the RWM model is used 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. 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 movements model with a steady-state distribution.

All simulations were performed for 1,000 simulation seconds. A pause time of 20 simulation seconds is fixed 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.

In our simulation, two cases are considered: mobile replica and static Replica. In the mobile Replica case, one benign node is used and one compromised node along with its replica as claim generators. Furthermore, these three nodes' initial placements are randomly chosen and their movements are randomly determined by the RWM model with a steady-state distribution. In the static Replica case, one compromised node is used along with its replica as claim generators. These two nodes do not move ,so fix their locations to the initial placements. By studying the static Replica case, how the distance between the compromised node and its replica affects the replica detection capability is investigated. The static replica case represents a strategic attacker and effectively the worst case for detection. The attacker keeps his nodes close together and immobile to lower the chance of detection. This also limits the attackers's effectiveness. In all scenarios, assume that all claims that have been forwarded to the base station reach it without any loss. We repeated each simulation scenario 1,000 times in such a way that the mobile nodes are initially placed in a different random location each time.

2) Simulation Results

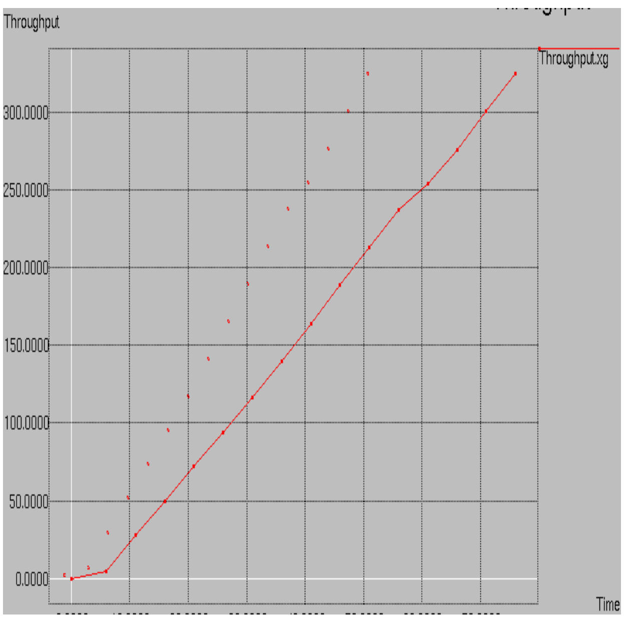


Fig- (1) Time vs throughput

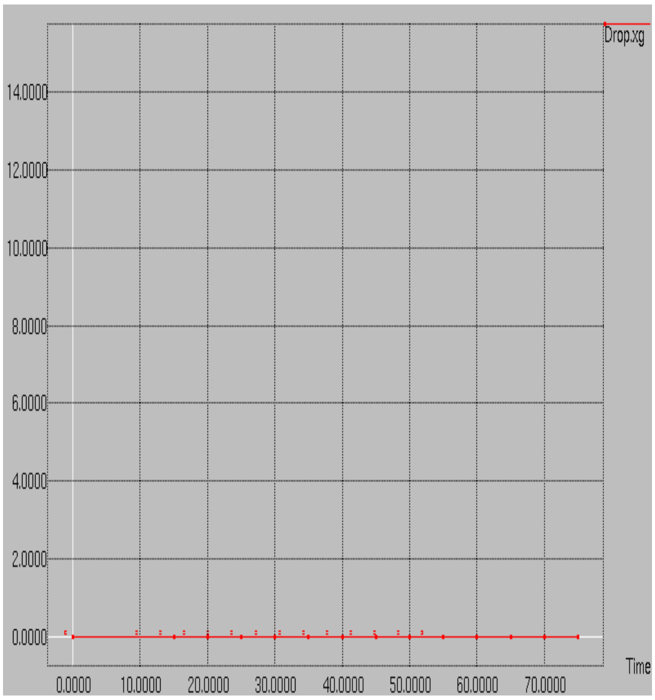


Fig - (2) Time vs drop

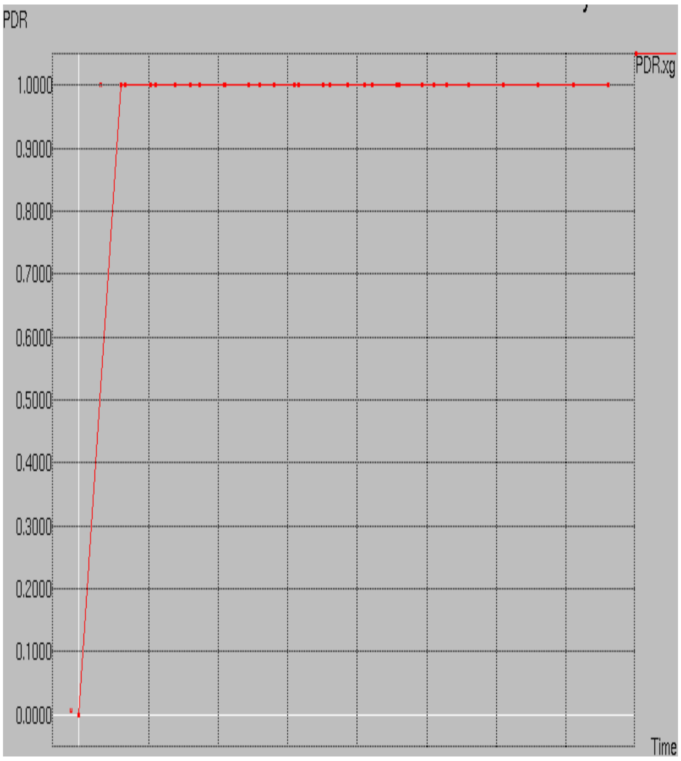


Fig- (3) Time vs Packet Delivery Ratio

5. CONCLUSIONS

In this paper, we have proposed a replica detection scheme for mobile sensor networks. We have analytically demonstrated the limitations of attacker strategies to evade our detection technique. In this scheme replica node disrupting the entire network operations is detected and revoked from the network quickly. The results of these simulations show that our scheme quickly detects mobile replicas with a small number of location claims.

6. FUTURE WORK

Mobile Replication Detection is based on the speed measurement in each and every node in the network. The replica attacker can allow his nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme. Replica nodes will appear to move much faster than benign node and thus their measured speeds will likely be over V max because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds V max, it is then highly likely that at least two nodes with the same identity are present in the network. In this phase, we address the problem of sensor node failure. When a sensor node fails because of energy depletion we need to choose alternative sensor for that particular region. We will fix energy threshold for each sensor, if it reaches that threshold it will inform the base station about the death. The base station should route another near-by energy-efficient sensor node to collect sensed data from that particular failed region.

7. REFERENCES

[1] 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.

[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] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan, "Fast

[5] 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,"

[7] .Proc.IEEE Symp.security and privacy,pp.49-63,May 2005.

[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] Engin Masazade,Ruixin Niu,Pramod K.Varshney and Mehmet Keskinoz,"Energy Aware Iterative Source Localization for Wireless Sensor Networks,"IEEE Transactions on signal Processing,vol 58,No.9,sep 2010.

[11] Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajal K. Das, Senior Member, IEEE, 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.