ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Efficient Detection of Node Replication Attacks in Mobile Sensor Networks

G.Raja[1], Dr.A.Rajesh[2]

Research Scholar, Department of CSE, St Peter's University, Chennai, India[1]

Professor & Head, Dept. of CSE, C.Abdul Hakeem college of Engineering and Technology,Vellore, Tamilnadu, India[2]

ABSTRACT: Wireless sensor networks are often deployed in hostile environments, where an adversary can physically capture some of the nodes. Once a node is captured, the attacker can re-program it and replicate the node in a large number of replicas, thus easily taking over the network. The detection of node replication attacks in a wire- less sensor network is therefore a fundamental problem. Compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented. Moreover, while most of the existing schemes in static networks rely on the witness-finding strategy, which cannot be applied to mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks incurs efficiency and security problems. In this paper Localized algorithms are proposed to resist node replication attacks in mobile sensor networks. The Merits of proposed algorithms are, it can effectively detect the node replication in localized manner. These algorithms are, also avoid network-wide synchronization and network-wide revocation.

Keywords:- Replication attack, security, wireless sensor networks, localized detection.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. A WSN can be deployed in harsh environments to fulfill both military and civil applications. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. For instance, an adversary could eavesdrop on all network communications and could capture nodes thereby acquiring all the information stored within (sensors are commonly assumed not to be tamper proof). Note that 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*. A cloned node has legitimate information (codes and key materials), it may participate in network operations in the same way as a non-compromised node; hence cloned nodes can launch a variety of attacks. For instance, a cloned node may create a black hole, initiate a wormhole attack with a collaborating adversary, inject false data or aggregate data in such a way to bias the result. Further, if data confidentiality is an issue, cloned nodes can violate this requirement leaking data. Recently, due to advances in robotics, mobile sensor networks have become feasible and applicable. Nevertheless, although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks. Even worse techniques used in detecting replicas in static environments are not useful in identifying replicas in mobile environments. With the consideration of nodes' mobility and the distributed nature of sensor networks, it is desirable, but very challenging, to have efficient and effective distributed algorithms for detecting replicas in mobile sensor networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

II.RELATED WORKS

The witness-finding strategy exploits the fact that one sensor node cannot appear at different locations, but, unfortunately, the sensor nodes in mobile sensor networks have the possibility of appearing at different locations at different times, so the above schemes cannot be directly applied to mobile sensor networks. Slight modification of these schemes can be helpful for applicability to mobile sensor networks. For instance, the witness-finding strategy can adapt to mobile environments if a timestamp is associated with each location claim. In addition, setting a fixed time window in advance and performing the witness-finding strategy for every units of time can also keep witness-finding feasible in mobile sensor networks. Nevertheless, accurate time synchronization among all the nodes in the network is necessary. Moreover, when witness-finding is applied to mobile sensor networks, routing the message to the witnesses incurs even higher communication cost. After identifying the replicas, a message used to revoke the replicas, possibly issued by the base station or the witness that detects the replicas, is usually flooded throughout the network. Nevertheless, network-wide broadcast is highly energy-consuming and, therefore, should be avoided in the protocol design. Time synchronization is needed by almost all detection algorithms. Nevertheless, it is still a challenging task to synchronize the time of nodes in the network, even though loose time synchronization is sufficient for the detection purpose. Hence, as we know that time synchronization algorithms currently need to be performed periodically to synchronize the time of each node in the network, thereby incurring tremendous overhead, it would be desirable to remove this requirement. Witness-finding could be categorized as a strategy of cooperative detection; sensor nodes collaborate in certain ways to determine which ones are the replicas. In this regard, the effectiveness of witness-finding could be reduced when a large number of sensor nodes have been compromised, because the compromised nodes can block the message issued by the nodes near the replicas. Hence, the witness nodes cannot discover the existence of replicas. To cope with this issue, localized algorithms could enhance the resilience against node compromise. In spite of the effectiveness in detecting replicas, all of the schemes adopting witness-finding have the common drawback that the detection period cannot be determined. In other words, the replica detection algorithm can be triggered to identify the replicas only after the network anomaly has been noticed by the network planner. Therefore, a detection algorithm that can always automatically detect the replica is desirable. Since the existing algorithms are built upon several other requirements, we have found that the common weakness of the existing protocols in detecting node replication attacks is that a large amount of communication cost is still unavoidable.

Challenges faced

- The most existing algorithms used only static network.
- Time synchronization is must.
- High communication cost is unavoidable.

III. THE PROPOSED METHOD

To detect the node replicas in mobile sensor networks using two localized algorithms, XED and EDD, are proposed. The proposed techniques develop solutions, challenge-and-response and encounter-number, are fundamentally different from the others. The proposed algorithm can resist node replication attacks in a localized fashion. Compared to the distributed algorithm, nodes perform the task without the intervention of the base station. The localized algorithm is a particular type of distributed algorithm. Each node in the localized algorithm can communicate with only its one-hop neighbors. This characteristic is helpful in reducing the communication overhead significantly and enhancing the resilience against node compromise. This algorithm can identify replicas with high detection accuracy. The revocation of the replicas can be performed by each node without flooding the entire network with the revocation messages. The time of nodes in the network does not need to be synchronized.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

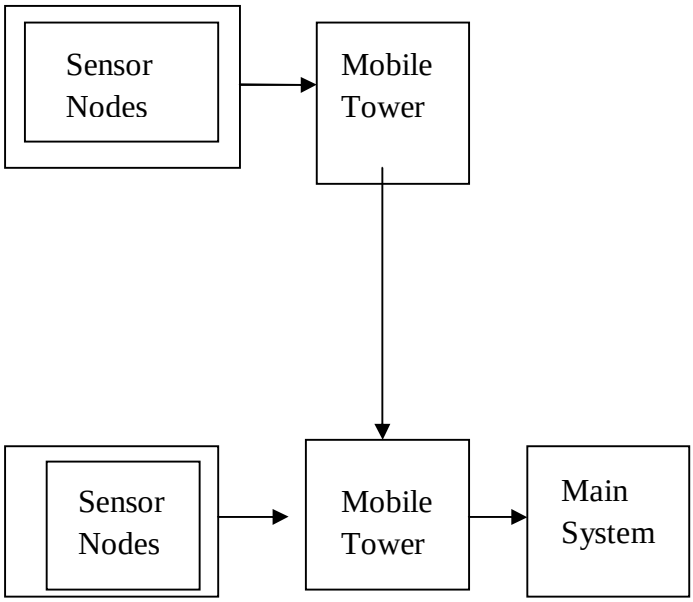

Fig. 1 Architecture

Node Deployment

Each node requests their node deployment to the base station at the time of deployment. After requesting, Node details are verified and save accordingly. Details include Node-Id, IP-Address and Port Number. Base station captures the node position and also save the node current position. Base station updates node position as per the node movement. Base station monitors the entire network and updates its position as per the movement.

Execute Offline Step

Execute localized algorithm's Offline steps. Algorithm generates the secret key and saves accordingly. The current node maintains other node's given secret key at the time of previous interaction. Current node maintains the black list also. The black list consists of replicated node details.

Find Next Hop and Candidate Hop

Based on sensor node's geographic position and destination node's (Main system) geographic position prepare the neighbor list to avoid opposite direction nodes. Neighbor list consist of current coverage's all the node. Prepare next hop and candidate list based on the neighbor list. Next hop is selected from neighbor list based on the destination node nearby hop balanced node is added to candidate list. The candidate list is used when current next hop is any problem (For example at the time of replication detection next hop is any problem furthermore candidate list is considerable.) the next priority is given to candidate hop. If more than one candidate is available the higher priority is goes to nearby source node position.

Localized Detection

After getting next hop name, execute proposed algorithm's online steps. In that algorithm first check next hop is sink node or not, if yes object will directly forward to sink node. Current hop check the received secret key is matching to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

previously given. If yes, then current node made communication to next hop and replace the existing secret key in next hop otherwise it is replicated node. The current next hop name is added to the current sensor nodes black list. Otherwise check current node already met the next hop or not, if yes request the secret key given during previous interaction.

Eliminate Replicated Hop

In localized detection find any replicated node, eliminate the replicated hop and select another next hop from candidate list. Again execute the localized algorithm. This process is made up to reach the original hop.

Advantages

- Localized Detection
- Efficiency and Effectiveness
- Network-Wide Revocation Avoidance
- Time Synchronization Avoidance

IV.CONCLUSION

Each and every sensor node sensing the data and send it to main system. Normally in mobile sensor network data transfer to hop by hop at that time any replicated node can act as original node, XED and EDD algorithms are used to find and avoid it. After detecting the replication node, that ID is added into black list and then find another hop from the candidate list and execute online algorithm, the condition is satisfied made communication with next hop otherwise added into black list. In addition the detecting replication node will eliminate from the entire networks.

REFERENCES

[1]. M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication at- tacks in wireless sensor networks," in *Proc. ACM Int. Symp. Mobile AdHoc Networking and Computing (MobiHoc)*, Montreal, Canada, 2007, pp. 80–89.
[2]. M. Conti, R. D. Pietro, and A. Spognardi, "Wireless sensor replica detection in mobile environment," in *Proc. Int. Conf. Distributed Computing and Networking (ICDCN)*, Hong Kong, China, 2012, pp.249–264.
[3]. G. Cormode and S. Muthukrishnan, "An improved data stream summary the count-min sketch and its applications," *J. Algorithms*, vol.55, no. 1, pp. 56–75, 2005.
[4]. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.
[5]. T. Karagiannis, J. L. Boudec, and M. Vojnovic, "Power law and expo- nential decay of inter contact times between mobile devices," in *Proc.ACM Int. Conf. Mobile Computing and Networking (MobiCom)*, Mon- treal, Canada, 2007, pp. 183–194.
[6]. M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in *Proc. Int. Conf. Infor- mation Processing in Sensor Networks (IPSN)*, Cambridge, MA, USA,2007.
[7]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node repli- cation attacks in sensor networks," in *Proc. IEEE Symp. Security and Privacy (S&P)*, Oakland, CA, USA, 2005, pp. 49–63.
[8]. J. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM)*, Brazil, 2009, pp.773–1781.
[9]. K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in *Proc. IEEE Int. Conf.Computer Communications (INFOCOM)*, San Diego, CA, USA, 2010, pp. 1–9.
[10]. M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor net-works," in *Proc. IEEE Int. Conf. Network Protocols (ICNP)*, Princeton, NJ, USA, 2009, pp. 284–293.

BIOGRAPHY

Raja G is a Research Scholar in the Computer Science Department, St.Peter's university, Chennai. He received Master of Technology (M.Tech) degree in 2010 from SRM University, Chennai, India. His research interests are Networks Security (wireless Networks), Mobile sensor Network, Information security