Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.600 – 603

RESEARCH ARTICLE

Detection of Mobile Replica Nodes in Wireless Sensor Networks

KARTHIK.S[1], K.P. KALIYAMURTHIE[2]

[1]Department of Information Technology, Bharath University, India

[2]Department of Information Technology, Bharath University, India

Abstract— In wireless sensor networks (WSN), there are many nodes and they are unattended so an adversary can easily capture and compromise the sensor nodes and take secret key from the nodes then make many replicas (duplicate) of them. After getting the secret key from the sensor node the sensitive data which is present in the nodes get leaked so an adversary can quickly degrades the network communication. To avoid this node compromised attack we use sequential probability ratio testing (SPRT). In literature several compromised node detection works well in static sensor networks and they do not work well in mobile sensor networks. Using SPRT we detect the compromised node in mobile sensor networks. This paper show analytically and through ns2 simulation experiments that the scheme detects duplicate node in an efficient and robust manner.

Key Terms: - mobile sensor nodes; static sensor networks; mobile sensor networks; network communication; sensitive

I. INTRODUCTION

A wireless sensor network consists of hundreds or even thousands of small nodes which are distributed over the network. These nodes sense the sensitive data from the location and send the sensitive message to the base station. The base station will verify the data and ID which is send by the sensor nodes[6]. These sensor nodes are deployed in hostile environment and the nodes are unattended which makes an adversary to compromise the sensor nodes and make many replicas of them. These replica nodes are dangerous to the network communication. Advances in robotics develop a variety of new architectures for autonomous wireless sensor networks. Mobile nodes in network communication are useful for network repair and event detection. These advanced sensor network architecture could be used in variety of application including intruder detection, border monitoring, and military patrols. The compromised mobile nodes inject the fake data and disrupt network operations and eavesdrop on network communications.

The dangerous attack is the compromised node attacks in which the adversary takes the secret keying materials from a compromised node, and generates large number of attacker controlled replicas throughout the network. An adversary can take the single sensor ID and make many replicas of them [7]. The time and effort needed to inject these replica nodes into the network should be much less than the effort to capture and compromise the equivalent number of original nodes. The replica nodes are controlled by an adversary. A solution to stop replica node attacks is to prevent the adversary from extracting the secret key materials from the mobile nodes by using temper resistant hardware, which makes significantly harder and more time consuming.

Software based replica detection schemes have been proposed for static sensor networks. The sensor nodes also report the location claims that identify their positions and send to the base station. In this paper, we proposed compromised node detection scheme based on the sequential probability ratio test (SPRT) [7]. A

benign node should never move at speeds in excess of system configuration speed. The benign mobile node should be always nearly or less than the system configuration speed. An uncompromised node should never move in excess of threshold value. In wireless sensor networks the compromised nodes have same ID present in the network which moves greater than the threshold value, which is taken as a duplicate node.

In literature some protocols are used to find the replica detection which are centralized protocol and distributed protocol. In centralized protocol there only central base station present in the network all the nodes which are present in the networks may communicate with the single base station. If the base station fails the whole network gets failed but in distributed protocol each and every node act as a base station if any of the node gets failed the node will take care of network. In centralized detection the single base station will verify the whole network operation and also it validates the messages which are send by the sensor nodes. The sequential probability ratio testing is come under centralized detection scheme. SPRT is a hypothesis testing method which contains null hypothesis and alternate hypothesis. An uncompromised node is taken as a null hypothesis and a compromised node is taken as an alternate hypothesis.

II. WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) consists of spatially distributed autonomous sensor to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi- hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding

The main characteristics of a WSN include: Power consumption constrains for nodes using batteries or energy harvesting, Ability to cope with node failures, Mobility of nodes, Communication failures, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Ease of use, Power consumption. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components.

III. ADVERSARY ENVIRONMENT

An adversary can eavesdrop on the communication, perform traffic analysis of the observed network behavior, adversary replay old messages or inject false messages into the network. Possible are also other types of attacks that aim violating Availability (denial-of-service attacks) like jamming the wireless channel. In WSNs these attacks can be particularly important as they can cause rapid battery draining and effectively disable individual sensor nodes or entire parts of a WSN. While there are many techniques known from other areas of security, the ability of an attacker to access (and eventually change) the internal state of a sensor node seems particularly characteristic for sensor networks. Depending on the WSN architecture, node capture attacks can have significant impact. Thus, most existing routing schemes for WSNs can be substantially influenced even through capture of a minute portion of the network, which enables secure and authenticated communication between the sensor nodes by means of a network-wide shared master key, capture of a single sensor node suffices to give the adversary unrestricted access to the WSN[1]. Most current security mechanisms for WSNs take node capture into account. It is usually assumed that node capture is “easy”. Thus, some security mechanisms are verified with respect to being able to resist capture of 100 and more sensor nodes out of 10,000 nodes.

IV. DUPLICATE NODE DETECTION

The nodes which are captured by an adversary can compromise the sensor nodes and make many replicas of them. These compromised nodes all have the same ID are present in the network[6]. To understand the dangers of node compromise, we must first define what we mean by node compromise. Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a myriad of attacks on the network. The attacker may also simply extract information vital to the network's security such as routing protocols, data, and security keys. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

A node compromise attack often consists of three stages. The first stage is physically obtaining and compromising the sensors; the second stage is redeploying the compromised nodes back to the sensor network; and the last stage is compromised sensors rejoining the network and launching attacks. So for all the proposed compromise detection schemes address the node compromise problem at the third stage based on node misbehavior detection. In this paper, we make three contributions. First, we make the first effort to address the node compromise problem at the second stage. Compromised nodes may be identified at the redeployment stage and prevented from rejoining the network. We refer to this as the node redeployment detection problem. Note that we are not aiming at completely solving the node compromise problem by our scheme alone. Instead, our goal is to prevent compromised nodes from easily rejoining the network.

Even when compromised nodes have bypassed our defense, we still have the traditional node compromise detection schemes as the second line of defense. Our second contribution is formalizing the node redeployment detection model, by exploiting the property of a stationary sensor network where the distance between two nodes does not change over time. The change of distance often indicates that the node is redeployed. Third, we propose two sets of solutions to detect node redeployment: a neighborship-based approach and a distance based approach, both of which work in a localized and distributed fashion. In the first approach, the redeployment detection is based on the change of neighborship. In the second approach, the redeployment detection is based on the change of distances. The technique of unpaired observations is used to detect the distance change. Our simulation results indicate that our proposed schemes can effectively detect node redeployment.

Random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation.

If the walk reaches or exceeds the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. We believe that SPRT is well suited for tackling the mobile replica detection problem in the sense that we can construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node; the lower and upper limits are properly configured to be associated with the shortfall and excess of the maximum speed of the mobile node, respectively. We apply SPRT 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 SPRT by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node; it will expedite the random walk to hit or cross the upper limit and thus lead to the base station accepting the alternate hypothesis that the mobile node has been replicated. On the other hand, each time the maximum speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus lead to the base station accepting the null hypothesis that mobile node has not been replicated. Once the base station decides that a mobile node has been replicated, it initiates revocation on the replica nodes. The false positive and false negatives are minimized using SPRT a hypothesis testing method that can make decisions quickly and accurately. In null hypothesis the mobile nodes are not been replicated but in alternate hypothesis the nodes get replicated. If the alternate hypothesis is accepted the replicated nodes are revoked from the network.

Using ns2 simulator the nodes are created. Initially the nodes are deployed in the network after deploying the nodes the base station sends the coverage region to all the nodes. Then the sensor nodes gather the data and sent to base station, the base station verifies the data. If the data gets dropped then the nodes won't send the data to the base station otherwise the replicated nodes send the false data to the base station. The functionality replica nodes disrupt the network operations. Using the sensor node speed we can detect the replica node. If the sensor node speed is within than the system configuration speed than that node is take as a uncompromised node. If the node speed is greater than the system configuration speed that node is taken as a compromised node and if any of the node is death in the particular location the neighbor node will take care of that particular region and sense the data and finally secure communication takes place initially the nodes are deployed in the hostile environment after deploying the nodes the base station send the coverage region to all the nodes in the network. Then the nodes gather the data and send to the base station if any of the node get drops the data or it sent the false data then the functionality of replica nodes takes place. Using the hypothesis testing method the replica nodes are detected. If null hypothesis is accepted then the replica nodes are detected and revoked from the network.

With the help of the ns-2 network simulator we simulate the proposed mobile replica detection scheme in a mobile sensor network. In our simulation, 200 mobile sensor nodes are placed within a square area of 250 m x 250 m. We use the Random Waypoint Mobility (RWM) model to determine mobile sensor node movement patterns. The trace file is also used to send the request packets to all the nodes in the network. Using this RWM the nodes moves for 0.05ms. 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 movement's 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 ranges is 50 m.

V. CONCLUSION

This paper concludes that the duplicates nodes in wireless sensor networks are detected by using a new statistical testing technique called sequential probability ratio testing. Using this technique the compromised sensor nodes are detected efficiently in mobile sensor networks.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

