Fake Data Termination in Wireless Sensor Networks

M.S. Pavithraa, C.Balakrishnan

Abstract— Wireless sensor networks are specified ad-hoc networks. They are characterized by their limited computing power and energy constraints because they are generally limited in memory, power and computational ability. Thus they can only transmit data to a limited distance. The major challenges of wireless sensor networks are security. This paper proposes a study of security in this kind of network. Here a list of attacks with their specificities and vulnerabilities are presented. Based on the location information presence of fake data can be identified. Here a solution to terminate this fake information is discussed.

Index Terms— Ad-hoc networks, sensor networks, attacks, security.

.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. For instance, an adversary could snoop on all network communications and could capture nodes thereby acquiring all the information stored within. 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.

Mobile nodes, essentially small robots with sensing and wireless communications are useful for tasks such as static sensor deployment, adaptive sampling, network repair, and event detection. These advanced sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The attacker may be able to capture and compromise mobile nodes, and then use them to inject facke data, disrupt network operations, and eavesdrop on network communications. In this scenario, a particularly dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker-controlled replicas that share the compromised node's keying materials and ID, and then spreads these replicas throughout the network. One of the solutions for the detection of node replication attacks relies on a centralized base station. In this solution, each node sends a list of its neighbors and their claimed locations (i.e., the geographic coordinates of each node) to a Base Station (BS). A voting mechanism is used within a neighborhood to agree on the legitimacy of a given node. However, applying this kind of method to the problem of replica detection, fails to detect clones that are not within the same neighborhood.

In order for a location claim to travel from source to destination node, it must pass through several intermediate nodes: gives a claim message path. Moreover, every node that routes this claim message will check the signature, store the message, and check for coherence with the other location claims received within the same iteration of the detection protocol. Node replication is eventually detected by the node (called witness) on the intersection of two paths that originate from networks.

The adversary can then leverage this insider position in many ways. For example, he can simply monitor a significant fraction of the network traffic that would pass through these nodes. Alternately, he could jam legitimate signals from benign nodes or inject falsified data to corrupt the sensors' monitoring operation. A more aggressive attacker could undermine common network protocols, including cluster formation, localization, and data aggregation, thereby causing continual disruption to network operations.

II. TYPES OF ATTACKS

A. Confidentiality

These attacks attempt to intercept private information sent over wireless associations, whether sent in the clear or encrypted by higher layer protocols.

To overcome this attack, the nodes in the wireless sensor network should not leak its sensed parameters to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.

B.Integrity

These attacks send forged control, management or data frames over wireless to mislead the recipient or facilitate another type of attack (e.g., DoS).

If the network is implemented with the confidentiality, an adversary may be unable to steal information. However, this doesn't mean that the data is safe. In such cases, the adversary may change the data, so as to send the sensor network into disarray of information.

Manuscript Received on May 05, 2012.

Ms. M. S. Pavithraa, (M.E), Department of the PG studies in Engineering, S.A. Engineering College, Chennai-77, Tamil Nadu, India.

Mr. C. Balakrishnan, M.E (Ph.D.) AssistantProfessor,Department of PG studies in Engineering, S.A. Engineering College,Chennai-77,TamilNadu,India.

C.Authentication

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services.

Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

D.Availability

These attacks impede delivery of wireless services to legitimate users, either by denying them access to WLAN resources or by crippling those resources. It is costly affair to adjust the traditional encryption algorithms to fit within the wireless sensor network. Some approaches choose to modify the code to reuse as much code as possible.

In case of wireless sensor networks usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, spoofed, replayed again or vanished. In this type of attack, the attacker has high processing power and large communication range. This type of attack may be prevented by data aggregation and authentication techniques.

III. SENSOR NODE COMMUNICATION

The robotics made it possible to develop a variety of new architectures for autonomous wireless networks of sensors. Enabling the nodes to encrypt, decrypt, and authenticate all of their communications as if they were the original captured node. Sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the security of unattended mobile nodes is extremely critical. It will first describe the detection accuracy of our proposed scheme and then present attack scenarios to break this scheme and a defense strategy

A. Neighbor node detection

In two-dimensional mobile sensor network the sensor nodes freely roam throughout the network. It assumes that every mobile sensor node's movement is physically limited by the system-configured maximum speed. This communication model is common in the current generation of sensor networks. Every mobile sensor node is capable of obtaining its distance information. And it also assumes that the nodes in the mobile sensor network communicate with a base station. Ever sensor node to detect the neighbor node based on distance and range of network as showed in Fig.1.

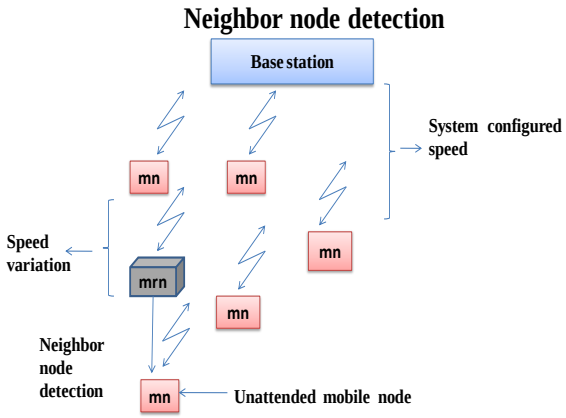

Fig.1

B. Data communication

Each time a mobile sensor node moves to a new location, it first discovers its set of neighboring nodes, time and location can consider both randomly generated It also assumes that all direct communication links between sensor nodes are bidirectional. Normal data communication is to communicate a particular node where the data was send from one node to another after the usage of encryption and decryption format using Elliptic curve cryptography algorithm. Normal data communication refers to unidirectional transformation of information to the destination but Attack data communication is sending the same data for 'n' number of times from different location at speed as shown in Fig.2.

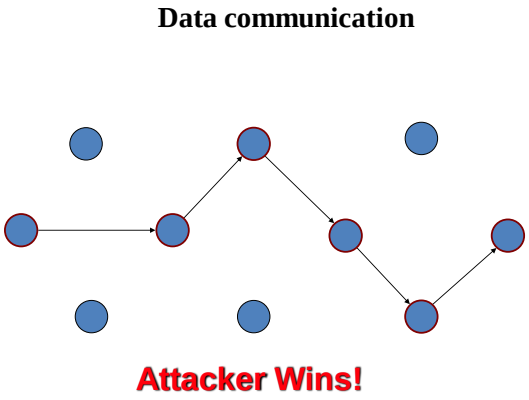

Fig.2

IV. FAKE NODE DETECTION

A dynamic authentication in the primary security enables existing nodes to authenticate new incoming nodes, triggering the establishment of secure links and broadcast authentication between neighboring nodes. This primary security design prevents intrusion from external malicious nodes

using the authentication scheme. For advanced security design, the intrusion detection system can exclude internal compromised nodes, which contains alarm return, trust evaluation, and black/white lists schemes.

The "random trip", a generic mobility model for independent mobiles that contains as special cases: the random waypoint on convex or non convex domains, random walk with rejection or wrapping, city section, space graph and other models. In static sensor networks, a sensor node is regarded as being replicated if it is placed in more than one location. 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. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network.

The sensor network has number of sensor nodes with IDs. The communication is assumed to be symmetric. In addition, each node is assumed to periodically broadcast a beacon containing its ID to its neighbors. This is usually required in various applications, for example, object tracking. After the nodes are deployed to the sensing field, the time is divided into time intervals each of which has the same length.

Sensors are unattended for longer period because they may be deployed in remote. Due to unattended operation following problems arise:

A. Exposure to Environmental Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and different environmental conditions. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

B. Managed Remotely

Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

C. No Central Management Control

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

V. APPLICATIONS

Wireless sensor networks have found their way into a wide variety of applications and systems with vastly varying requirements and characteristics. As a consequence, it is becoming increasingly difficult to discuss typical requirements regarding hardware issues and software support. A classification of sample applications according to the design space is presented, considering deployment, mobility, resources, cost, energy, heterogeneity, modality, infrastructure, topology, coverage, connectivity, size, lifetime and QoS.

Centralized processing the environment model is very computational intensive; it usually runs on a central server and process data gathered from the sensor network. High data volume for example, nautical X-band radar can generate megabytes of data per second. QoS sensitivity it defines the utility of the data, there is an engineering trade-off between QoS and energy constraint.

A. Structure Health Monitoring (SHM) System

The widely accepted goals of SHM system include detecting damage, localizing damage, estimating the extent of the damage and predicting the residual life of the structure

B. Smart Energy

Societal-scale sensor network can greatly improve the efficiency of energy-provision chain, which consists of three components, the energy-generation, distribution, and consumption infrastructure.

C. Home Applications and Office Applications

The electronic appliances enter average household, great commercial opportunities exist in home automation, smart home/office environment.

VI. CONCLUSION

The lifetime of wireless sensor network is limited due to use of some kind of battery. To be able to reduce the energy consumption and so improve the lifetime of wireless sensor network that consists of different methods that has been developed in last few years. Sensor networks offer countless challenges, but their versatility and their broad range of applications are eliciting more and more interest from the research community as well as from industry. Sensor networks have the potential of triggering the next revolution in information technology. This paper gives overview of wireless sensor networks, their security issues and some applications of wireless sensor network need a secure communication.

REFERENCES

1. J.-Y.L. Boudec and M. Vojnovi_c, "Perfect Simulation and Stationary of a Class of Mobility Models," Proc. IEEE INFOCOM, pp. 2743-2754, Mar. 2005.
2. 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.
3. M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized,Efficient, and Distributed Protocol for the Detection of NodeReplication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.
4. K. Dantu, M. Rahimi, H. Shah, S. Babel, A.Dhariwal, and G.S.Sukhatme, "Robomote: nabling Mobility in Sensor Networks,"Proc. Fourth IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 404-409, Apr. 2005.
5. 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.
6. 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.
7. L. Hu and D. Evans, "Localization for Mobile Sensor Networks," Proc. ACM MobiCom, pp. 45-57, Sept. 2004.
8. 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.
9. A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Seventh IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 245-256, Apr. 2008.
10. S. PalChaudhuri, J.-Y.L. Boudec, and M. Vojnovi_c, "Perfect Simulations for Random Trip Mobility Models," Proc. 38th Ann.Simulation Symp., Apr. 2005.
11. 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.
12. H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor etworks," Ad Hoc Networks, vol. 5, no. 1, pp. 112-125, Jan. 2007.
13. K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security (CCS), pp. 264-271, Oct. 2006.

AUTHOR PROFILE

Mr. C.BalaKrishnan is working as Assistant Professor, Department of PG studies in Engineering, S.A.Engineering College, Chennai, Tamilnadu, India. He has completed BE Electronics and Communication Engineering in Mysore University in the year 1991 and completed M.E Computer Science and Engineering in Madras Institute of technology, Anna University in the year 2008. He is at the verge of completion of Doctoral degree in Security in Wireless Networks in Anna University, Chennai. His research areas are Network Security, Network & management and Adhoc networks. Topics he is the member of ISTE.

M.S. Pavithraa received the bachelor's degree in 2009 in Computer Science and Engineering from Anna University in Vel multitech Engineering. She is currently doing Master's degree in computer science & engineering from Anna University in S.A Engineering College. Her research interests include wireless sensor networks, database technology, and network security. Topics she is a member of the IEEE.