Security in Wireless Sensor Networks

Mudit Rathore[1], Sindhu Kesaboina[2], Sairaj[3], and Aditya Kumawat[4]

[1]Indian Institute of Information Technology Allahabad, ICM2015502
[2]Indian Institute of Information Technology Allahabad, ICM2015004
[3]Indian Institute of Information Technology Allahabad, ICM2015006
[4]Indian Institute of Information Technology Allahabad, ICM2014001

***Abstract*— Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article, we present a survey of security issues in WSNs.**

I. INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security, and social factors. The basic idea of the sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring, etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties.[1]

In the case of a wireless sensor network, the communication among the sensors is done using wireless transceivers. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus.

While some aspects of WSNs are similar to traditional wireless ad hoc networks, important distinctions exist which greatly affect how security is achieved. The differences between sensor networks and ad hoc networks are[2]:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed. Sensor nodes are densely deployed.
- Sensor nodes are prone to failures due to harsh environments and energy constraints.
- The topology of a sensor network changes very frequently due to failures or mobility.
- Sensor nodes are limited in computation, memory, and power resources.
- Sensor nodes may not have global identification

These differences greatly affect how secure data-transfer schemes are implemented in WSNs. For example, the use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service attacks.

II. BACKGROUND

A. Components of a Sensor Node

A WSN is usually composed of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts[2]:

- a sensing unit
- a processing unit
- a transceiver unit
- a power unit

It may also have additional application-dependent components such as a location finding system, power

generator, and mobilizer (Fig. 1). Sensing units are usually composed of two sub units: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells).

Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Finally, a mobilizer may sometimes be needed to move the sensor node, depending on the application

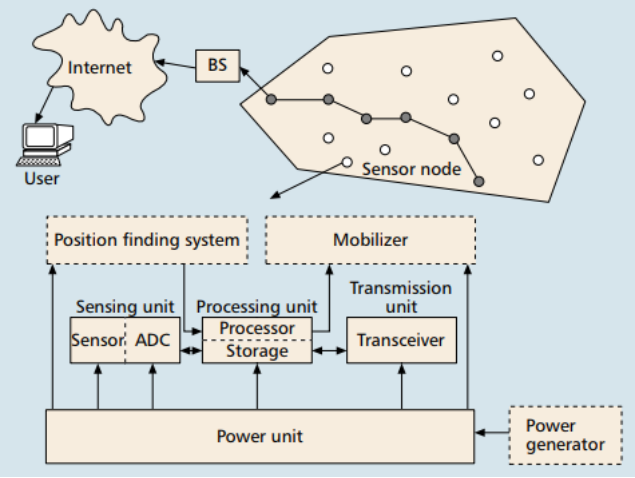

Fig. 1. Components of a sensor node

B. Protocol Stack

The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [2]:

- Physical layer: responsible for frequency selection, carrier frequency generation, signal deflection, modulation, and data encryption
- Data link layer: responsible for the multiplexing of data streams, data frame detection, medium access, and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections
- Network layer: responsible for specifying the assignment of addresses and how packets are forwarded
- Transport layer: responsible for specifying how the reliable transport of packets will take place
- Application layer: responsible for specifying how the data is requested and provided for both individual sensor nodes and interactions with the end user

C. Constraints in WSNs

Individual sensor nodes in a WSN are inherently resource constrained. They have limited processing capability, storage capacity, and communication bandwidth. Each of these limitations is due in part to the two greatest constraints — limited energy and physical size. The design of security services in WSNs must consider the hardware constraints of the sensor nodes:

- Energy: energy consumption in sensor nodes can be categorized into three parts:
  - Energy for the sensor transducer
  - Energy for communication among sensor nodes
  - Energy for microprocessor computation

  The study in [3, 4] found that each bit transmitted in WSNs consumes about as much power as executing 800–1000 instructions. Thus, communication is more costly than computation in WSNs. Further, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions.
- Computation: the embedded processors in sensor nodes are generally not as powerful as those in nodes of a wired or ad hoc network. As such, complex cryptographic algorithms cannot be used in WSNs.
- Memory: memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There is usually not enough space to run complicated algorithms after loading OS and application code. This makes it impractical to use the majority of current security algorithms.
- Transmission range: the communication range of sensor nodes is limited both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather and terrain.

III. Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbe-

havior. The security requirements in WSNs include:

- Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks
- Authorization, which ensures that only authorized sensors can be involved in providing information to network services
- Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node
- Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients
- Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
- Non-repudiation, which denotes that a node cannot deny sending a message it has previously sent

IV. Security Threats and Issues in WSNs

Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks.

A. Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

1) Denial of Service: Denial of Service (DoS) [3], [4] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

2) Sybil Attack: In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 1). This type of attack where a node forges the identities of more than one node is the Sybil attack [5], [6]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [6]. Basically, any peer–to–peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols.

3) Blackhole/Sinkhole Attack: In this attack, a malicious node acts as a blackhole [7] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations.

4) Hello Flood Attack: Hello Flood Attack is introduced in [8]. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop–class attacker in [8]) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while

sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

5) Wormhole Attack: Wormhole attack [9] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

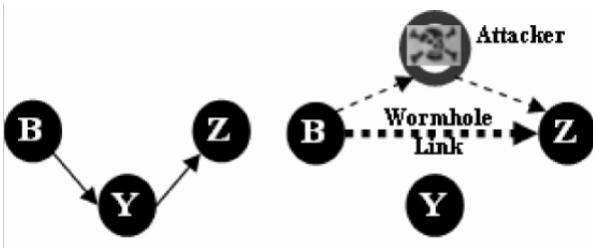

Fig. 2. Wormhole attack left(a) right(b)

Figure (a and b) shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

V. Security Mechanisms

The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level and low-level.

A. Low-level mechanisms

Low-level security primitives for securing sensor networks includes,

- Key establishment and trust setup
- Secrecy and authentication
- Secure routing
- Resilience to node capture

1) Key establishment and trust setup: The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. In addition, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme.[10]

2) Secrecy and authentication: Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. Cryptography is the standard defense. Remarkable system trade-offs arise when incorporating cryptography into sensor networks. For point-to-point communication[12], end-to-end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast.

3) Secure routing: Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denialof-service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. [11]

4) Resilience to node capture: One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defense, but it's expensive, since current technology does not provide a high level of security. Algorithmic solutions to the problem of node capture are preferable.[10]

B. High-Level Mechanisms

High-level security mechanisms for securing sensor networks include secure group management, intrusion detection, and secure data aggregation.

1) Secure group management: Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group. [10]

2) Intrusion detection: Wireless sensor networks are susceptible to many forms of intrusion. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.[10]

3) Secure data aggregation: One advantage of a wireless sensor network is the finegrain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured.[11]

VI. Summary

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless adhoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

References

[1] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[2] I. F. Akyildiz et al., "A Survey on Sensor Setworks," IEEE Commun.Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.

[3] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26-36.

[4] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 - 904.

[5] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[6] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 - 268.

[7] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 - 688.

[8] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[9] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 - 1986.

[10] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[11] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006

D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, year 2005.