Wireless Sensor Networks and Security Challenges

Yogesh Kumar
(Sr. Lecturer, CSE Deptt., B.P.R College of Engg., Gohana
Rajiv Munjal
(Lecturer, CSE Deptt., B.P.R College of Engg., Gohana)
Krishan Kumar
(Lecturer, CSE Deptt., B.P.R College of Engg., Gohana)

ABSTRACT
Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced.

Keywords-
Wireless Sensor Network; Security Goal; Security Attacks; Defensive mechanisms; Challenges.

1. INTRODUCTION

Basically, sensor networks are application dependent. Popular wireless sensor network applications include wildlife monitoring, bushfire response, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates etc. Majority of the sensor network are deployed in hostile environments with active intelligent opposition. Hence security is a crucial issue. Less obvious but just as important security dependent applications include:

• Disasters: In many disaster scenarios, especially those induced by terrorist activities, it may be necessary to protect the location of casualties from unauthorized disclosure

• Public Safety: In applications where chemical, biological or other environmental threats are monitored, it is vital that the availability of the network is never threatened. Attacks causing false alarms may lead to panic responses or even worse total disregard for the signals.

• Home Healthcare: In such applications, privacy protection is essential. Only authorized users should be able to query and monitor the network.

This paper includes has been organized in following sections. Section 2 gives the information about the security goals in Wireless Sensor Networks. Security attacks and their classification are discussed in section 3. Section 4 discusses about the various security mechanisms. Major challenges faced are given in Section 5 followed by the conclusion section.

2. SECURITY GOALS FOR SENSOR NETWORKS

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary [5]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization.

3. ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks. [4] Figure1 shows the classification of attacks under general categories and Figure 2 shows the attacks classification on WSN.

A. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

1) Attacks against Privacy

The main privacy problem is not that sensor networks enable the collection of information. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks [8] against sensor privacy are:

• **Monitor and Eavesdropping:** When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the

eavesdropping can act effectively against the privacy protection.

• **Traffic Analysis**: Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns.

• **Camouflage Adversaries**: One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

B. Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature. Routing Attacks in Sensor Networks, Denial of Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering etc.

4. SECURITY MECHANISM

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. Figure 3 shows the order of security mechanisms.

A. Low-Level Mechanism

Low-level security primitives for securing sensor networks includes, Key establishment and trust setup, Secrecy and authentication, Privacy Robustness to communication denial of service, Secure routing, Resilience to node capture etc.

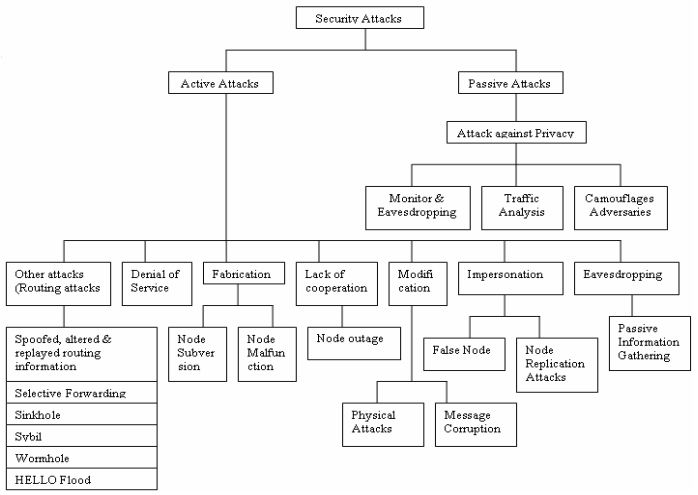

Figure 1: General Classification of Security Attacks

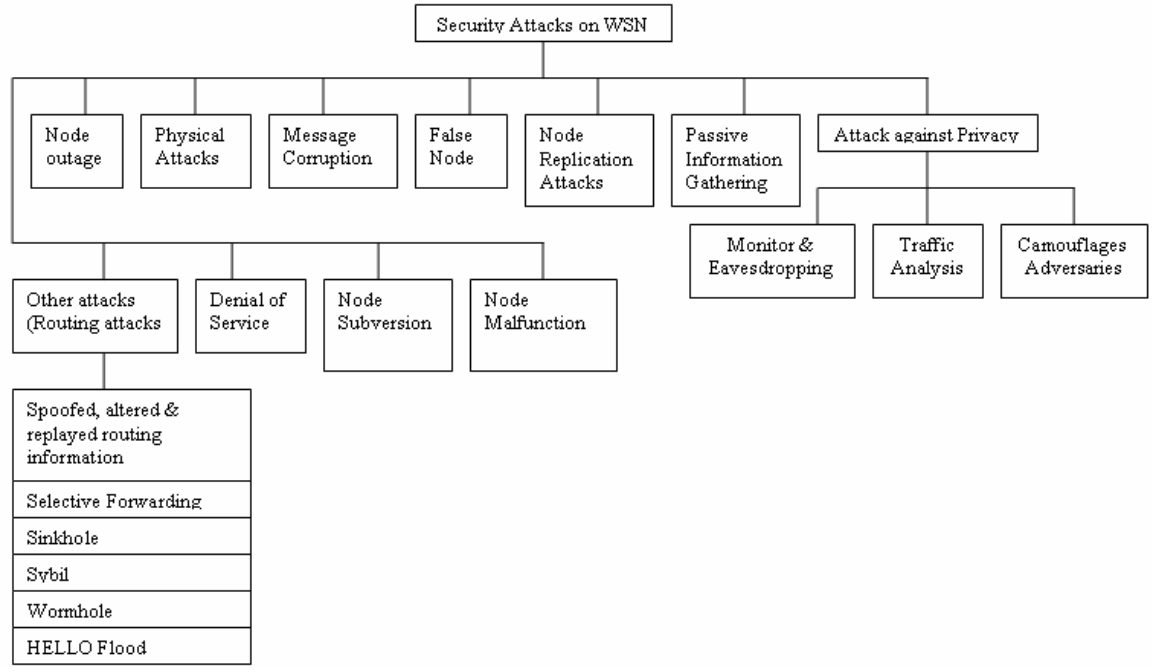

Figure 2: Classification of Security Attacks on WSN

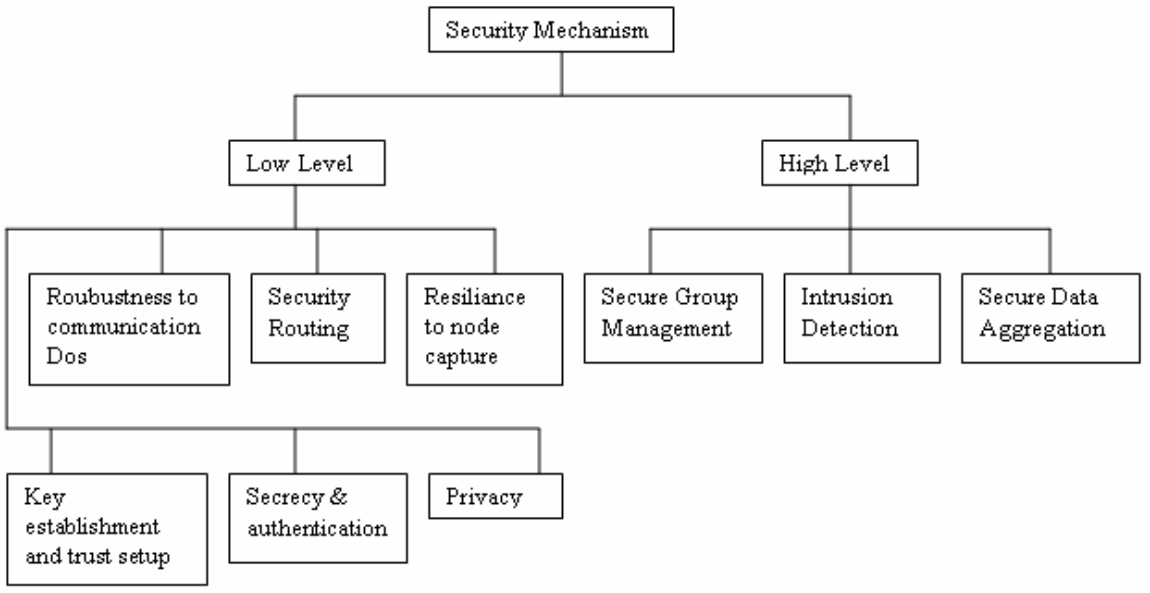

Figure3: Security mechanisms

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. [6]

3) Privacy

Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important. [1]

4) Robustness to communication denial of service

An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to send signal.[1]

5) 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 denial of-service attacks on the routing protocol, preventing communication.[2]

6) 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. [1]

B. High-Level Mechanism

High-level security mechanisms for securing sensor networks, includes 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. 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. [1]

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.[1]

3) Secure data aggregation

One advantage of a wireless sensor network is the fine grain 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.[6]

5. CHALLENGES OF SENSOR NETWORKS

A wireless sensor network is a special network which has many constraint compared to a
traditional computer network.

A. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes
eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary.[7]

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self configuration. Security schemes must be able to operate within this dynamic environment.[3]

C. Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices.

D. Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. [5]

E. Immense Scale

Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

F. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.[5]

• Unreliable Transfer: Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.

• Conflicts: Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.

• Latency: The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

G. Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes [5]:

• Exposure to Physical Attacks: The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The probability 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.

• Managed Remotely: Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.

• No Central Management Point: 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. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

6. CONCLUSION

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 ad-hoc 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.

7. REFERENCES

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

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003

[4] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[6] 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

[7] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009

[8] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002

[9] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006

[10] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, year 2009

[11] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[12] 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.