Wireless Sensor Network Security Challenges and Attacks: A Review

Navjot Sidhu[1], Monika Sachdeva[2] and Krishan Kumar[3]
[1]*Department of Computer Engineering,*
Punjab Technical University, Jalandhar, Punjab
[2,3]*Department of Computer Science & Engineering,*
Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab
E-mail: [1]navjotsidhu8@gmail.com, [2]monika.sal@rediffmail.com, [3]k.salujasbs@gmail.com

***Abstract*—Wireless Sensor Networks are a special type of Ad-hoc networks. Although these networks are quite popular now-a-days but limited computing power, energy constraints and security are major challenges for these networks. This paper presents a review on Wireless Sensor Networks and their key challenges. A detailed review of various vulnerabilities and security attacks is also presented. Finally a layer-wise classification of these attacks is also summarized.**

Keywords: Wireless Sensor Networks, Security, Attacks, Protocols, Vulnerabilities

I. INTRODUCTION

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, and multifunctional sensor nodes [1]. These tiny nodes consist of sensing, data processing, and communicating components. A sensor network is composed of a large number of sensor nodes, which are densely deployed. The sensor network possesses a self organizing capabilities and processing abilities. These features ensure a wide range of applications for sensor networks. Some of the application areas of sensor networks include health e.g. tracking and monitoring doctors and patients, and drug administration in hospitals, military applications, e.g., for battlefield surveillance, reconnaissance of opposing forces and terrain and battle damage assessment, security applications and some other commercial applications like environment control, managing inventory control and vehicle tracking and detection etc.

Although Wireless Sensor Networks are a part of Traditional Ad-hoc Networks. Both of these networks share some common features as Self-organization, energy efficiency, wireless multi-hop. But still there are some key differences between sensor networks and ad hoc networks. Some of the important differences are outlined below [1]–[2]:

Sensor nodes are limited in computation, memory, power resources, and communication speed or bandwidth as compared with ad hoc nodes:

1. The number of sensor nodes in a sensor network can be several times more than the nodes in an ad hoc network.
2. The Wireless Sensor Network has one base station, which has more computing capabilities and act as the controller of the network.
3. Sensor nodes are densely deployed as compared to ad-hoc nodes.
4. Sensor nodes are prone to failures due to various environmental conditions.
5. The topology of a sensor network changes very frequently due to the node failure, joining or mobility.
6. Wireless Sensor Networks are much application specific as compared to ad-hoc networks.

II. SENSOR NODE AND ITS CONSTRUCTION

A Sensor node in Wireless Sensor Network is a node that is capable of gathering, processing the sensory information and also communicating that information with other nodes connected to it in a network. Huge variations, in the design of sensor devices, are being available. Most sensor devices must have the following hardware:

1. A micro-controller for computation,
2. A small RAM for dynamic data,
3. One or more flash memories to hold the program code and long-lived data,
4. A wireless transceiver,
5. An antenna,
6. An analog-to-digital converter,
7. One or more sensors,
8. And a power source

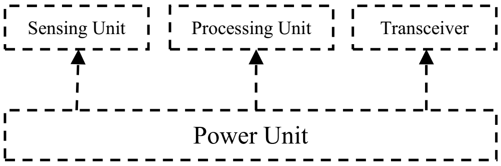

Fig. 1 Components of a Sensor Node

In the end, a sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit.

Sensing Unit is composed of two sub-units: Sensors and analog-to-digital converters. Sensors sense the phenomenon and send the observed analog signals to analog-to-digital converters to convert signals in digital form and further send them to processing unit. The processing unit has a small storage unit and manages the procedures to process the sensed information from one or more nodes. A transceiver connects the node to the network. The most important component of sensor node is Power unit which may be supported by some powerful scavenging unit. There can be some other application dependent subunits like location finding system to find the location, mobilize to move sensor nodes when it is required [1].

III. Challenges of Wireless Sensor Network

In sensor networks, wireless nodes self organizes themselves with a dynamic topology. As the number of nodes in a typical sensor network is much higher and to ensure coverage and connectivity, dense deployments are often desired. Sensor nodes have very limited energy, which make them prone to failure. Ideally, sensor network should be power-efficient, small, inexpensive and reliable. According to [3] the key challenges of wireless sensor network are:

1. *Lifetime:* Lifetime is an extremely critical factor and its limiting factor is the energy consumption of sensor nodes. Energy consumption could be reduced by considering the interdependence between individual layers in the network protocol stack.
2. *Flexibility:* Sensor networks should be scalable, i.e. they should be able to adapt dynamic changes to the network. E.g. sensor nodes should adapt changes in the topology, due to failure of some nodes.
3. *Maintenance:* Maintenance in a sensor network leads to complete or partial update of the sensor node program.
4. *Data Collection:* For data collection, sensor network can use ubiquitous mobile agents that randomly move and gather data from sensor nodes and access points. As all data are relayed to a base station, but this form of data collection may affect the lifetime of the network. So, an interesting solution is clustering, which divides network into many clusters. In each cluster, a cluster head collects data from other node and transmits this data to other clusters. The main objective of this technique is to extend the lifetime of the network by limiting number of communications.
5. *Power:* Sensor network use tiny sensors with low computing power, which make them incapable to use complex algorithms. If a sensor node has o do many calculations, its responsiveness will significantly deteriorates.

III. Routing and Data Transmission Mechanism

The sensor nodes usually scattered in field with the capabilities to collect data and send to the sink i.e., a base station. Various protocols are used by sink and other sensor nodes in order to communicate successfully with each other. The protocol stack of wireless sensor networks consists of Application Layer, Transport Layer, Network Layer, Data Link Layer and Physical layer [1]. Each Layer performs a variety of functions, so that data transmission, between tiny sensor nodes, becomes possible. Table 1 represents the different layers of the protocol stack, their functions and protocols used at each layer.

TABLE 1 PROTOCOLS USED AT DIFFERENT LAYERS

LAYER	TASK PERFORMED	PROTOCOLS USED
Application Layer	• Use various application software for Sensing	• Sensor Management Protocol (SMP) • Task Assignment and Data advertising Protocol (TADAP) • Sensor query and data dissemination protocol (SQDDP)
Transport Layer	• Maintain the flow of data	• User Datagram Protocol (UDP) • Transmission Control Protocol (TCP)
Network Layer	• Provide Route to the data supplied by the transport layer • Provide internetworking	• Small Minimum Energy Communication Network Protocol (SMECN) • Sensor protocols for information via negotiation (SPIN) • Sequential assignment routing (SAR) • Low-energy adaptive clustering hierarchy (LEACH)
Data Link Layer	• Provide power awareness and minimize collision	• Media access Control (MAC)
Physical Layer	• Provide robust modulation, transmission and receiving techniques	• Use schemes for frequency selection, carrier frequency generation, signal detection, modulation and data encryption

IV. Vulnerabilities and Attacks

Due to various key challenges like limiting energy, low power, lifetime etc., wireless sensor networks are vulnerable to many threats. Most of these attacks affect limiting energy of sensor networks [4].

A. *Classification of WSN Attacks*

Generally, attacks are classified as either passive or active depending upon the action they perform. According to [5] attack can be defined as an action to get illegal access to a service, information or to integrity, confidentiality, or availability of a system. In case of wireless sensor networks, attack can be one of the following types:

1. *Passive*: An attack that does not modify data only monitors the communication and threatens the confidentiality.
2. *Active*: An attack that modify and delete existing data and threatens the confidentiality, authentication and data integrity.
3. *Insider*: Steal key information and run malicious code by compromising authorized or legitimate nodes of the network.
4. *Outsider*: Attacker has no particular access to the network.
5. *Mote-Class*: Attacker has access to the minority nodes with similar capabilities.
6. *Laptop-Class*: Attacker has access to powerful devices such as laptop, capable processors, greater battery power and high power antenna.

B. Principles of WSN Security

Security principles of wireless sensor networks can be classified as [5]:

1. *Authentication*: defines that data is originated from the authorized source.
2. *Confidentiality*: defines that only authorized sensor nodes can access the messages.
3. *Integrity*: defines that any message has not been modified during transmission by unauthorized node.
4. *Availability*: defines that services provided by wireless sensor network or by a single sensor node must be available whenever necessary.
5. *Data Freshness*: defines that no old data have been used.

C. Current WSN Attacks

Wireless sensor networks are vulnerable to security attacks due to the broadcast nature of transmission, limiting energy or nodes are often placed in a dangerous environment. In many applications, the data obtained by the sensing nodes needs to be kept confidential. In the absence of security measures a false or malicious node could intercept private information or send false information to sensor nodes in the network [6]. The brief overview of current wireless sensor network attacks is given below [4], [6], [7]:

1. Eavesdropping: It is a passive attack which only listen the network to intercept information, but does not modify data. That’s why, it is very difficult to detect.
2. *Radio Jamming*: An attacker sends the radio waves at the same frequency that is used by other authorized sensor nodes of the network.
3. *Message Injection*: It is an active attack, in which aim of the attacker is to send the false messages on the network to corrupt the records or to saturate the network.
4. *Message Replication*: It is also an active attack, here attacker catches the transmitted packets over the network and sends those packets to wrong nodes of the network.
5. *Node Destruction*: It is a type of physical attack in which ne or many nodes of sensor network are destroyed, making network not to work to destroy a node the link two nodes. In this type of attack, the attacker can also reprogram the sensor nodes.
6. *Denial of service*: This is another active attack which makes the wireless sensor network out of order by sending large amounts of data to the sensors to be active and consumes their energy.
7. *Hello Flooding*: With an attack of Hello flooding, an attacker can use a device with large enough transmission power for compromising every node in its neighbour.
8. *Black Hole Attack*: In black hole attack, at first a malicious node is inserted into the network. This malicious node changes the routing tables of the network. The aim is to force a maximum of neighbouring nodes to send data to it. Once it captures all sent data, it does not forward or replies back.
9. *Gray Hole Attack*: It is a variant of the black hole attack. In this attack the malicious node replays all information concerning the route and non critical data. That’s why this attack is more difficult to detect.
10. *Wormhole Attack*: Unlike the black hole attack, this attack needs to insert in the network at least two malicious nodes. These nodes are connected by powerful connection. This attack wrongs the other nodes of the network and proposes a quicker path. Nodes choose this shortest path to send their data, and in actual they send their data to malicious nodes.
11. *Sinkhole Attack*: In this attack the malicious node attacks directly the data, which circulate near the sink i.e. base station. To perform this attack, the malicious node offers the quickest path to reach the sink. All nodes, which are near the malicious node, send data for the sink which may be captured by the attacker.
12. *Sybil Attack*: In Sybil attack, a malicious sensor which is masquerading as multiple sensors, modifies the routing table.
13. *Message Alteration*: A malicious node catches a message and changes it, by adding wrong information or deleting some information.
14. *Slowdown*: An attacker can make use of malicious nodes to slow down the network. This attack prevents a sensor to sleep in different ways, in order to consume its battery quickly.

V. Layer-wise Classification of Attacks

A Wireless Sensor network is comprised of a large number of sensors that collaboratively monitor various environments. To collect data from WSNs, base stations and aggregation points are commonly used. As they usually have more resources than normal sensor nodes. Security is one of the most important aspects that deserve great attention [7].

TABLE 2 Layer-wise Classification of Attacks

LAYER	THREAT	COUNTERMEASURES
Application Layer	• Selective Message Forwarding • Data Aggregation Distortion	• Integrity Protection • Confidentiality Protection
Transport Layer	• Flooding	• Manage connection Request
Network Layer	• False Routing • Message Replication • Black Hole • Sink Hole • Selective Forwarding • Worm Hole • DOS • Sybil Attack	• Routing Access Restrictions • False Routing Information Detection • Wormhole Detection
Data Link Layer	• Traffic Manipulation • Identity Spoofing	• Misbehavior Detection • Identity Protection
Physical Layer	• Eavesdropping • Radio Jamming • Node Destruction	• Access Restriction • Encryption

Table 2 presents, a classification of attacks based on the layering model of Open System Interconnection, along with some potential countermeasures [5]–[8].

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of networks, unknown topology prior to deployment, and high risk of physical attacks, it is a challenge to provide security in Wireless Sensor Networks. The Wireless Sensor Network has general security requirements of availability, integrity, authentication, confidentiality and non-repudiation. These security requirements can be provided by distribution mechanisms with the requirement of scalability, efficiency key connectivity and resilience [8].

VI. Conclusion

Recent micro-electro-mechanical system advances have allowed use multifunctional sensor networks. But information in these networks is still not secure and vulnerable to many attacks. Communications over wireless channels are insecure and easily susceptible to various kinds of attacks. It is impractical to protect each individual sensor node from physical or logical attack. The security and vulnerabilities of a wireless sensor network depend upon the particular application for which sensor network is deployed. Most of the attacks in wireless sensor networks are caused by inserting false or wrong information by malicious nodes within the network.

Presented classifications are crucial for future implementation of Wireless Sensor Networks.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: a survey”, Elsevier Science Computer Networks, vol. 38, pp. 393–422, 2002.

[2] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor Network Security: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, pp. 52-73, 2009.

[3] D. Puccinelli and M. Haenggi, “Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing”, IEEE Circuits and System Magazine, pp. 19-29, 2005.

[4] D. Martins and H. Guyennet, “Wireless Sensor Network attacks and Security Mechanisms: a Short Survey”, Proceedings of 13th IEEE International Conference on Network-Based Information Systems, pp. 313-320, 2010.

[5] H. Modares, R. Salleh and a. Moravejosharish, “Overview of Security Issues in Wireless Sensor Networks”, Proceedings of 3rd IEEE International Conference on Computing Intelligence, Modelling & Simulation, pp. 308-311, 2011.

[6] K. Sharma and M.K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Spacial Issue on MANETs, pp. 42-45, 2010.

[7] K. Xing, S.S. R. Srinivasan, M. Rivera, J. Li and X. Cheng, “Attacks and Countermeasures in Sensor Networks: A Survey”, Network Security, Springer, pp. 1-28, 2005.

[8] Z.S. Bojkovic, B.M. Bakmaz and M.R. Bakmaz, “ Security Issues in Wireless Sensor Networks”, International Journal of Communications, Issue 1, vol. 2, pp. 106-115, 2008.

[9] S. Raman, A. Prakash, K.B. Pulla and P. Srivastava, “Wireless sensor networks: A Survey of Intrusion and their Explored Remedies”, International Journal of engineering Science and Technology, vol. 2(5), pp. 962-969, 2010.

[10] A.K. Pathan, H. Lee and C.S. Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, ICACT, pp. 1043-1048, 2006.

[11] J. zheng and A. Jamalipour, “Wireless Sensor Networks-A Netwoking Perspective”, John Wiley, 2009.

[12] H. Suo, J. Wan, L. Huang and C. Zou, “ Issues and Challenges of Wireless Sensor Networks Localization in Emerging Applications”, Proceeding of IEEE International Conference on Computer Science & Electronics Engineering, pp. 447-451, 2012.

[13] G. Padmavthi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” International Journal of Computer Science and Information Security, vol. 4, pp. 1-9, 2009.

[14] T. Kavitha and D. Sridharan, “Security Vulnerabilities in Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security 5, pp. 31-44.

[15] X. Chen, K. Makki, K. Yen and N. Pissinou, “Sensor Network Security: A Survey”, IEEE Communication Surveys & Tutorials, vol. 11, no. 2, pp. 52-73.

[16] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Elsevier Ad-hoc networks, pp. 293-315, 2003.