International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 2; March 2018; Page No. 1277-1281

Security issues in wireless sensor network: A review

Munisha Devi
Research Scholar, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract
WSNs applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion. 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. Wireless Sensor networks consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. Due to the reason that the sensor nodes are highly distributed, there is a need of security in the network. Security is an important issue nowadays in almost every network. There are some security issues and many attacks that need to be look around and work upon. Finally, this paper discusses on some defensive measures of WSN giving focus on the key management, link layer and routing security.

Keywords: wireless sensor networks, security concerns, attacks

Introduction
Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it. These nodes consist of three main components-sensing, data processing and communication. Various applications of WSN includes habitat monitoring, manufacturing and logistics, environmental observation and forecast systems, military applications, health, home and office application and a variety of intelligent and smart system. Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. For example, when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic [1] Providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations [2]. A security scheme in WSNs must provide efficient key distribution while maintaining the ability for communication between all relevant nodes. In addition to key distribution, secure routing protocols must be considered. These protocols are concerned with how a node sends messages to other nodes or a base station. A key challenge is that of authenticated broadcast [3, 4]. Existing authenticated broadcast methods often rely on public key cryptography and include high computational overhead making them infeasible in WSNs. Secure routing protocols proposed for use in WSNs, such as SPINS [5], must consider these factors. Additionally, the constraint on energy in WSNs leads to the desire for data aggregation. This aggregation of sensor data needs to be secure in order to ensure information integrity and confidentiality [6, 7]. In Section 2 we discusses about the security issues that arise in WSN because of its resource restrictions, In Section 3 we focuses on the essential requirements for ensuring WSN security, Section 4 briefly describes soame attacks at different layers and some proposed countermeasures and Section 5 discusses about the defensive measures of WSN directing two important security aspects which are cryptography and key management.

Security Issues
Limited Resources
All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

Limited memory and storage space
A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

Power Limitation
Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that

security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

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.

Unreliable Transfer
Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

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. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem [8].

Security Requirements
Wireless Sensor Network is vulnerable to various attacks like any other conventional network, but its limited resource characteristics and unique application features requires some extra security requirements including the typical network requirements. The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSNs include:

A. Data Authenticity
Only providing data confidentiality is not enough to ensure the data security in WSN. As an adversary can change messages on communication or inject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. *Data Integrity*
Provision of data confidentiality stop s the outflow of information, but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data integrity can be provided by Message Authentication Code (MAC).

B. Data Confidentiality
Confidentiality is an acceptance of authorized access to information communicated from a certified sender to a certified receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. For secure co mmunication, encryption is used. Data is encrypted with a secret key that only authorized users have. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks.

C. Availability
We can not ignore the importance of availability of nodes when they are needed. For example, when WSN is used for monitoring purpose in manufacturing system, unavailability of nodes may fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to fulfil the functionality of the network. As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable. So, security policies should be implied so that sensor nodes do not try to allocate extra resources for security purpose.

D. Self Organization
A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations.

E. Freshness
Data freshness ensures that the data communicated is recent and no previous messages have been replayed by an adversary. Data freshness is classified into two types based on the message ordering; weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand, gives complete request-response pair and allows the delay estimation. Sensor measurements require weak freshness, while strong freshness is needed for time synchronization within the network. For ensuring the freshness of a packet, a timestamp can be attached to it.

Security Attacks
WSNs are vulnerable to various types of attacks. According to the security requireSecurity is one of the major aspects of any system. Traditional WSNs are Security is one of the major aspects of any system. Traditional WSNs are affected by various types of attacks. Theseattacks can be categorized as:
1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. In silent attacks, the attacker compromises a sensor node and feeds wrong data. Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs.

A. Physical Attack
This attack is also known as node capture. In this type of

attack, attackers gain full control over some sensor nodes through direct physical access [11]. The attacker can abstract source code which ultimately provides attacker the information about the network that can alter the code to get admittance into the network. As the cost of sensor nodes must be kept as cheap as possible for WSN, Sensor nodes with tamper proofing features are impractical. This is why sensor nodes are susceptible to be physically being accessed. Physical attacks have significant impacts on routing and access control mechanisms of WSN.

B. Attacks at Different Layer

Besides physical attack, adversaries perform a large number of attacks remotely. These attacks take place affecting different networking layers of WSN. This subsection describes some of these well known attacks

Physical Layer

Physical layer is responsible for actual data transmission and reception, frequency selection, carrier frequency generation, signalling function and data encryption [9]. This layer also addresses the transmission media among the communicating nodes. WSN uses shared and radio based transmission medium which makes it susceptible to jamming or radio interference.

Jamming

Jamming is one of the basic yet destructive attacks that attempt to interrupt in physical layer of the WSN structure.In physical layer, jamming is a common attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN. This radio signal interferes with other signal sent by a sensor node and the receivers within the range of the attacker cannot receive any message.

Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel.

Collision

Collision is a type of link layer jamming that occurs when two nodes try to transfer data at the same time and at the same frequency [13]. In order to generate collision, the attacker listens to the transmissions in WSN. When he finds out the starting of a message, he sends his own radio signal for a small amount of time to interfere with the message [11] which causes CRC error at the receiving end. Because of this attack, the receivers cannot receive the message correctly

Network Layer

Network layer is responsible for routing messages from one to another node which are neighbours or may be multi hops away for example, node to base station or node to cluster leader. Network layer is exposed to different types of attacks such as selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding. There are several attacks exploiting routing mechanisms in WSN. Some familiar attacks are listed here.

Selective Forwarding

Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbour nodes. The impact becomes worse when these malicious nodes are at closer to the base station [12].

Then many sensor nodes route messages
through these malicious nodes. As a consequence of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring.

Sinkhole Attack

In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbours by spoofing or replaying an advertisement of high quality route to the base station [13]. The attacker can do any malicious activity with the packets passing through the compromised node.

Wormhole Attack

Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [14]. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally.

Sybil Attack

In Sybil attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [13]. In the location based routing protocols, nodes need to exchange location information with their neighbours to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place. Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN.

Transport Layer

In network layer end to end connections are managed.

Flooding Attack

According to [15] and [16], at this layer, adversaries exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node.

Research challenges of wireless networks

Since wireless devices need to be small and wireless networks are bandwidth limited, some of the key challenges in wireless

networks are data rate enhancements, minimizing size, cost, low power networking, user security and Quality of Service (QoS).

A. Signal Fading

Unlike wired media, signals transmitted over a wireless medium may be distorted or weakened because they are propagated over an open, unprotected, and ever changing medium with irregular boundary. Besides, the same signal may disperse and travel on different paths due to reflection, diffraction, and scattering caused by obstacles before it arrives at the receiver. The dispersed signals on different paths may take different times to reach the destination. Thus, the resultant signal after summing up all dispersed signals may have been significantly distorted and attenuated when compared with the transmitted signal. The receiver may not recognize the signal and hence the transmitted data cannot be received.

B. Mobility

To support mobility, an ongoing connection should be kept alive as a user roams around. In an infrastructured network, a handoff occurs when a mobile host moves from the coverage of a base station or access point to that of another one. A protocol is therefore required to ensure seamless transition during a handoff. This includes deciding when a handoff should occur and how data is routed during the handoff process. In some occasions, packets are lost during a handoff.

C. Power and Energy

A mobile device is generally handy, small in size, and dedicated to perform a certain set of functions; its power source may not be able to deliver power as much as the one installed in a fixed device.When a device is allowed to move freely, it would generally be hard to receive a continuous supply of power. To conserve energy, a mobile device should be able to operate in an effective and efficient manner.

D. Data Rate

Improving the current data rates to support future high speed applications is essential, especially, if multimedia service are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Therefore, it is imperative that manufacturers implement a well thought out design that considers these factors in order to achieve higher data rates. Data compression plays a major role when multimedia applications such as video conferencing are to be supported by a wireless network.

E. Security

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 801.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. In large enterprises, an IP network level security solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to make access to fixed access networks reliable. Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly.

F. (Quality of Service) QoS

Quality of Service is a measure of network performance that reflects the network's transmission quality and service availability. For each flow of network traffic, QoS can be characterized by four parameters: Reliability, Delay, Jitter, and Bandwidth.

There are several important issues related to QoS in wireless networks that do not get addressed in the wireline environment. These issues arise because wireless networks are inherently different from wireline networks. Several important wireless network characteristics include handoff, dynamic connections, and actuating transport QoS [11]. The traffic QoS parameters (throughput, delay and loss rate) are not sufficient in a wireless environment. In a wireline environment, the application layer can normally be assured that once a connection is established it will continue to exist until it is closed. In a wireless environment, connections may temporarily break during a process termed handoff. It is unlikely that handoff can take place without at least a short connection interruption. Applications running in a wireless environment must be able to recover from temporary interruptions, and should specify the maximum connection interruption time that they can tolerate. The application could specify such a time via a large loss rate; however, this would overload the meaning of loss rate. A maximum frequency of connection interruption is another performance parameter that would be valuable in a wireless network. Some applications may request a low interruption frequency so that the QoS perceived by the user remains satisfactory. A low interruption frequency implies that handoffs do not occur too often. Applications may accept a larger maximum connection interruption time in exchange for a low interruption frequency.

Conclusion

This paper gives an idea of a major subset of security problems that Wireless Sensor Network faces because of its exceptional design characteristics, communication and deployment pattern. At the same time, this paper includes brief discussion on the important security aspects that are required to design a secure Wire Sensor Network. There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network; some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Designing a secure WSN needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for WSN security. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of

these wireless sensor network applications. In particular, the addition of public key cryptography and the addition of public-key based key management.

References

1. Yong Wang. Garhan Attebury A survey of security issue in wireless sensor network IEEE Communications Surveys, • 2nd Quarter, 2006.
2. Chan H, Perrig A. Security and Privacy in Sensor Network IEEE Communications Surveys & Tutorials • 2nd Quarter, 2006.
3. Shi E, Perrig A. Designing Secure Sensor Networks, Wireless Commun. Mag. 2004; 11(6):38-43.
4. Akyildiz IF, *et al*., A Survey on Sensor Setworks, IEEE Commun. Mag. 2002; 40(8):102-114.
5. Perrig A, *et al*., SPINS: Security Protocols for Sensor Networks, Wireless Networks. 2002; 8(5):521-34.
6. Przydatek BD, Song, Perrig A. SIA: Secure Information Aggregation in Sensor Networks,
7. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine. 2002; 40(8):102-114.
8. Becher E, Benenson Z, Dornseif M. Tampering with motes: Real-world physical attacks on wireless sensor networks. In Proceeding of the 3rd International Conference on Security in Pervasive Computing, 2006, 104-118.
9. John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A survey. Security in Distributed, Grid, and Pervasive Computing, 2006.
10. Datema S. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology 2005.
11. Tanveer Z, Albert Z. Security issues in wireless sensor networks. In ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication, page 40, Washington, DC, USA, IEEE Computer Society, 2006.
12. Mayank Saraogi. Security in Wireless Sensor Networks. In ACM SenSys, 2004.
13. Wood AD, Stankovic JA. Denial of service in sensor networks, IEEE Computer. 2002; 35(10):54-62.
14. Khalil I, Bagchi S, Shroff NB. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. Comput. Netw. 2007; 51(13):3750-3772.
15. Wood A, Stankovic J. Denial of service in sensor networks. In Computer. 2002; 35:54U-62.
16. Raymond DR, Midkiff SF. Denial-of- service in wireless sensor networks: Attacks and defenses. In IEEE Pervasive Computing. 2008; 7:74-81.
17. Diffie W, Hellman ME. New Directions in Cryptography, IEEE Trans. Info. Theory. 1976; 22(6):644-54.
18. Rivest RL, Shamir A, Adleman L.A Method for Obtaining Digital Signatures and Public- Key Cryptosystems, Commun. ACM. 1983; 26(1):96-99.
19. Menezes AJ, Vanstone SA, Oorschot PCV, Handbook of Applied Cryptography, Boca Raton, FL: CRC Press, 1996.
20. Rivest RL. The RC5 Encryption Algorithm, Fast Software Encryption, B. Preneel (Ed.), Springer, 1995, 86-96.
21. Al-Karaki JN, Kamal AE. Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Wireless Commun. 2004; 11(6):6–28.