DIFFERENT INTRUSION AND ITS DETECTION OF WIRELESS SENSOR NETWORK: A REVIEW

Piyu Sarcar, Rimpi Datta and Abhijit Ghosh
Department of ECE, Narula Institute of Technology, Kolkata, India

ABSTRACT

Wireless Sensor Network (WSN) has become an emerging technology of wireless communication and computing. Wireless Sensor Network is a self-configured, infrastructure-less wireless network which comprises of a few to large number of spatially distributed autonomous sensor nodes and a base station. The function of the base station is to interface user and network. A sensor node combines hardware and software. The main deployment of sensor network is sensing, data processing and transmitting data. WSN has different application in enemy intrusion detection in the battlefield in the military application, medical field, atmospheric disaster, agricultural and industrial applications. In Wireless sensor network each node is a battery-operated low power device and operated in ad-hoc principle, which indicates network power is mainly dependent on rate of energy consumption. Ad-hoc networking nature of WSN allows the attacker for different types of attacks from passive eavesdropping to active attacks. As WSN requires hop by hop routing to transport the packets to the destination, any intermediate node acting maliciously can drop, modify or misguide the traffic traversing through it. Confidentiality, authenticity, integrity, data freshness and quality of service (QoS) are the most important issues for wireless sensor nodes. An attacker may collect and destroy sensitive information if the transmission is not properly encrypted. However, avoiding collision and providing cooperation among the nodes during the transmission are done by using medium access control protocols. This paper focuses on the security threats on the resource restricted design and deployment characteristics along with the requirements to design a secured WSN system. In this paper wormhole attacks, black hole attacks, Sybil attacks, hello flood attack, denial of service attacks and private attacks are investigated. In this paper different link layer attacks are also discussed. Not only does this document about the popular attacks in different layers of WSN, but also provides some remedies against these attacks.

Keywords: Authenticity, Confidentiality, Key Management, Security Risks, Wireless Sensor Network.
Cite this Article: Piyu Sarcar, Rimpi Datta and Abhijit Ghosh, Different Intrusion and its Detection of Wireless Sensor Network: A Review, *International Journal of Electronics and Communication Engineering and Technology*, 10(2), 2019, pp. 31-39. http://www.iaeme.com/IJECET/issues.asp?JType=IJECET&VType=10&IType=2

1. INTRODUCTION

Wireless Sensor Network consists of a number of sensor nodes which is arranged in ad hoc fashion which is deployed for sensing environmental phenomenon [1]. A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Initially, WSN was mainly used for military surveillance but now its application has moved to both civilian and commercial levels. Applications like environmental and medical monitoring, manufacturing machinery performance monitoring, home automation, and traffic control are facilitated by Wireless Sensor Networks.

In order to ensure the WSN’s application success, security is amongst the biggest concerns. For example, while using the WSN for military purpose, the most important task is to keep the received information confidential as well as authentic. Typically, a sensor network consists of a large number of tiny sensor nodes and a few powerful control nodes called base stations. A sensor node processor is of 4-8 MHz, having 4KB of RAM and 128KB flash, these nodes are supplied with limited battery power and have small memory and limited computational ability. Sometimes the sensor nodes are scattered unattended into the hazardous environment without appropriate infrastructure. These attributes of WSN make them more vulnerable, complicating the further development of security mechanisms. The unreliable channels adding up to the security issues of WSN. Such problems encourage the researchers to address the sensor network security on first priority and to develop security protocols and algorithms suitable for WSN. The design limitations, communication and deployment patterns of WSN impose several security problems making it vulnerable to different attacks. Using security loops, adversaries can perform different types of attacks to disrupt the network, hamper or misguide the communication flow of the network, or to intercept, or modify the confidential data. To counter against these attacks, coming from different levels of WSN security vulnerabilities, it is very important to know about the security requirements of WSN. Proper analysis of security requirements gives right directions to implement proper defenses against the security violations.

2. SECURITY PROBLEMS

Sensor networks are capable of interacting with the surrounding environment very closely, thus are exposed the hostile environment at the risk of physically being tampered. The sensor networks can work in an unattended or in the absence of any remote monitoring system. Also, there are lots of security issues related to Wireless Sensor Network that can be logically exploited by the adversaries to attack the networks. The security problems in WSN are as follows.

In Wireless Sensor Network, the sensor nodes themselves are points of attack which can be used by adversaries to subvert the sensor nodes to gain full control and disrupt the network [2]. If the sensor nodes are compromised then the attackers will be able to know all the confidential information stored in them and may launch a number of actions against the network by using these compromised nodes. For example, the compromised nodes may discard important data or report with wrong or modified data to mislead any decision taken based on this data.
The cryptographic key information may get released and the entire network may get compromised. Malicious nodes can be added to exhaust other sensor nodes, attract them to send data preventing the passage of true data.

The attackers can target the routing information as well which is used to maintain the communication between sensor nodes and the base station [3]. The routing mechanisms used for WSN requires complete trust amongst all the participating nodes. The proper transportation of data in the network depends upon the integrity of the routing information collected from other nodes. False routing information transmitted by a host may partition the network by misguiding the traffic to a small group of nodes and thus causes disruptions in communication. As WSN requires hop by hop routing to transport the packets to the destination, any intermediate node acting maliciously can drop, modify or misguide the traffic traversing through it. Adversaries can create these security problems in WSN by compromising nodes, or spoofing, altering, replaying the routing information.

The wireless channel, used as communication media, is unreliable and creates a lot of security issues. The adversary just needs to be in the radio range of the nodes and he can easily intercept or inject any message in the transmission data without causing any interruption in the network communication. Thus, an attacker may collect sensitive information if the transmission is not encrypted. However, avoiding collision and providing cooperation among the nodes during the transmission are done by using medium access control protocols.

3. SECURITY REQUIREMENTS
Similar to other conventional network, WSN is also vulnerable to a diverse range of attacks but its limited resources characteristics and unique features requires extra security requirements along with the typical network requirements.

3.1. Confidentiality
Sensor nodes communicate sensitive data, thus it is necessary to ensure that any intruder could not get confidential information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data.

3.2. Integrity
Providing data confidentiality is not enough to ensure the data security in WSN. 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 whereas data authentication ensures the receiver that the data has not been modified during the transmission.

3.3. Data Freshness
Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design.

3.4. Authentication
For WSN, network must be authenticated. Receiving node must be ensured that the packet comes from the reliable source and no packet is dropped or lost by the malicious nodes.
3.5. Non-Repudiation
It indicates that the source node sends all packet properly to the destination node and no packet is rejected to send.

4. ATTACKS
Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks [6], but also through traffic analysis, privacy violation, physical attacks, and so on.

4.1. The Sybil Attack
It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [5]. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities.

4.2. Wormhole Attack
A wormhole attack has more than one adversaries, which have better communication resources such as processing power, memory than legitimate nodes and it can establish better communication channel through tunnel [9]. In the wormhole attack, a malicious node tunnels messages from one part of the network over a low latency link to a different part. The tunnel may be established in three different ways, through an out-of-band hidden channel, packet encapsulation, or high-powered transmission.

Electronic copy available at: https://ssrn.com/abstract=3554193
4.4. Hello Flood Attack
When the sender is in the same radio range of the receiver, the malicious node illegally uses powerful transformer to make fool to the sender node and send a flood of fraud messages to the network to prevent other messages to be exchanged.

![Hello Flood Attack Diagram]

**Figure** Hello Flood Attack

4.5. Node Replication Attack
Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node replicated in this fashion can severely disrupt a sensor network’s performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

4.6. Black Hole Attack
The black hole attack is active attack which reduces the network efficiency. When a source node broadcasts for requesting route towards destination to transfer information, the malicious nodes falsifies the route so that the sender node cannot identify the genuine path and thus the packet is dropped.

![Black Hole Attack Diagram]

**Figure** Black hole attack

4.7. Denial of Service Attack
When attackers flood the large number of packets to the network, the network cannot sense all of the packet. Instead they denied the packet to forward and dropped. This types of attack is termed as denial of service attack. DoS attack is visible in physical layer, link layer, transport layer and application layer.
4.8. Privacy Attacks

Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, in the famous “panda-hunter problem”, the hunter can imply the position of pandas by monitoring the traffic.

Some of the more common attacks against sensor privacy are:

4.8.1. Monitor and Eavesdropping

This is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents. 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.

4.8.2. Traffic Analysis

Traffic analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified.

4.8.3. Camouflage

Adversaries can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets.

4.9. Link Layer Attacks

In the physical layer the attackers attack the legitimate node by tampering, eavesdropping and jamming. Black hole attack is mainly seen in network layers. In the link layer collision and exhaustion takes place. Flooding and de-synchronization are the main problems in transport layer.

5. DEFENSIVE MEASURES

Lots of research have been done and are ongoing to privilege the WSN with crucial security support. WSN needs effective, energy and resource efficient key management scheme for providing confidentiality, integrity and authentication security services [7].
Link layer security mechanism in WSN can provide important security support by guaranteeing integrity, authenticity, and confidentiality of messages because they deny an outsider access to the network. Secure routing is another essential requirement for protecting WSN against external and insider attack. Proper security solution for preventing DoS attacks at different layers is also a dire need for protecting the WSN from disruption.

5.1. Cryptography and Key Management

Wireless sensor networks are unique (among other embedded wireless networks) in this aspect due to their size, mobility and computational/power constraints. Indeed, researchers envision wireless sensor networks to be orders of magnitude larger than their traditional embedded counterparts. This, coupled with the operational constraints described previously, makes secure key management an absolute necessity in most wireless sensor network designs [4]. Because encryption and key management/establishment are so crucial for the defense of a wireless sensor network, with nearly all aspects of wireless sensor network defenses relying on solid encryption, we first begin with an overview of the unique key and encryption issues surrounding wireless sensor networks before discussing more specific sensor network defenses.

Key management issues in wireless networks are not unique to wireless sensor networks [8]. Indeed, key establishment and management issues have been studied in depth outside of the wireless networking arena. Traditionally, key establishment is done using one of many public-key protocols. One of the most common is the Diffie-Hellman public key protocol, but there are many others.

Most of the traditional techniques, however, are unsuitable in low power devices such as wireless sensor networks. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography. In this case, it is necessary to maintain two mathematically related keys, one of which is made public while the other is kept private. This allows data to be encrypted with the public key and decrypted only with the private key. The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network. This is true in the general case, however, show that it is feasible with the right selection of algorithms.

Symmetric cryptography is therefore the typical choice for applications that cannot afford the computational complexity of asymmetric cryptography. Symmetric schemes utilize a single shared key known only between the two communicating hosts. This shared key is used for both encrypting and decrypting data. The traditional example of symmetric cryptography is DES (Data Encryption Standard). The use of DES, however, is quite limited due to the fact that it can be broken relatively easily.

5.2. Link Layer Security

TinySec performs at link layer using cryptographic primitives—encryption and MAC. It supports two different security options: TinySec-AE and TinySec-Auth. In TinySec-AE, Tiny Sec encrypts the data payload and verify the packet with MAC [10]. With TinySec-Auth, the packet verification is performed with a MAC without encrypting the data payload. To protect data against jamming in the physical layer, the source node use admission control and mechanism which limits the transmission rate. To protect packet against wrong route generated by malicious node, a source node use multiple route to transfer packet because if one route fails to transfer data or misbehaving another route can transfer the packet correctly to the destination. To protect data against collision in the link layer we can use error correcting codes. Encryption can be used to protect data in the network layer [12].
6. SECURE ROUTING

Deng, Han, and Mishra describe an intrusion tolerant routing protocol, INSENS, that is designed to limit the scope of an intruder’s destruction and route despite network intrusion without having to identify the intruder. They note that an intruder need not be an actual intrusion on the sensor network, but might simply be a node that is malfunctioning for no particularly malicious reason. Identifying an actual intruder versus a malfunctioning node can be extremely difficult, and for this reason Deng et al. make no distinction between the two.

The first technique they describe to mitigate the damage done by a potential intruder is to simply employ the use of redundancy. In this case, as described previously under denial of service, multiple identical messages are routed between a source and destination. A message is sent once along several distinct paths with the hope that at least one will arrive at the destination. To discern which, if any, of the messages arriving at the destination are authentic, an authentication scheme can be employed to confirm the message’s integrity.

Deng et al. also make use of an assumed asymmetry between base stations and wireless sensor nodes. They assume that the base stations are somewhat less resource constrained than the individual sensor node. For this reason, they suggest using the base station to compute routing tables on behalf of the individual sensor nodes. This is done in three phases. In the first phase, the base station broadcasts a request message to each neighbor which is then propagated throughout the network. In the second phase, the base station collects local connectivity information from each node. Finally, the base station computes a series of forwarding tables for each node.

The forwarding tables will include the redundancy information used for the redundant message transmission described above. There are several possible attacks that can be made on the routing protocol during each of the three stages described above. In the first phase, a node might spoof the base station by sending a spurious request message. A malicious node might also include a fake path(s) when forwarding the request message to its neighbors. It may not even forward the request message at all.

To counter this, Deng et al. use a scheme similar to μTESLA where one-way key chains are used to identify a message originating from the base station. Tanachaiwiwat, et al. presented a novel technique named TRANS (Trust Routing for Location Aware Sensor Networks) [11]. The TRANS routing protocol is designed for use in data centric networks. It also makes use of a loose-time synchronization asymmetric cryptographic scheme to ensure message confidentiality. In their implementation, μTESLA is used to ensure message authentication and confidentiality. Using μTESLA, TRANS is able to ensure that a message is sent along a path of trusted nodes while also using location aware routing. The strategy is for the base station to broadcast an encrypted message to all of its neighbors. Only those neighbors who are trusted will possess the shared key necessary to decrypt the message. The trusted neighbor(s) then adds its location (for the return trip), encrypts the new message with its own shared key and forwards the message to its neighbor closest to the destination. Once the message reaches the destination, the recipient is able to authenticate the source (base station) using the MAC that will correspond to the base station. To acknowledge or reply to the message, the destination node can simply forward a return message along the same trusted path from which the first message was received. One particular challenge to secure routing in wireless sensor networks is that it is very easy for a single node to disrupt the entire routing protocol by simply disrupting the route discovery process.
7. CONCLUSION
In this paper we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, trust, denial of service, and so on. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher.

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 will likely make strong security a more realistic expectation in the future. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas.

REFERENCES

[1] F.Anjum, and P.Mouchtaris, (Security For Wireless Ad Hoc Networks.. Wiley, 2007)
[2] E.Becher, Z.Benenson, and M.Dornseif, Tampering with motes: Real-world physical attacks on wireless sensor networks. In Proceeding of the 3rd International Conference on Security in Pervasive Computing 104–118, 2006.
[3] D.R.Raymond, S.F.Midkiff, Denial-Of-Service In Wireless Sensor Networks: Attacks and defenses. In IEEE Pervasive Computing, volume 7, pages 74–81, 2008.
[4] D.Liu, P.Ning, R.Li, Establishing pair-wise keys in distributed sensor networks. ACM Transactions on Information Systems Security, Vol. 8, No. 1, 41-77, 2005.
[5] R.John, Douceur, The Sybil attack. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS ’02), Cambridge, 2002.
[6] A.Wood, J.Stankovic, Denial of service in sensor networks. In Computer, volume 35, 54-62, 2002.
[7] Z.Tanveer, Z.Albert, Security issues in wireless sensor networks. In ICSNC ’06: Proceedings of the International Conference on Systems and Networks Communication, Washington DC, USA, 40, 2006.
[8] W.Du, J.Deng, Y.S.Han, P.K.Varshney, A Key Pre Distribution Scheme For Sensor Networks Using Deployment Knowledge. IEEE Transactions on Dependable and Secure Computing, 3(1) 62–77, 2006.
[9] I.Khalil, S.Bagchi, N. B. Shroff, Liteworp: Detection and Isolation of The Wormhole Attack In Static Multihop Wireless Networks. Comput. Netw, 51(13)3750– 3772, 2007.
[10] R.Sokullu, I.Korkmaz, O.Dagdeviren, A.Mitseva, & N.R.Prasad, An Investigation on IEEE 802.15.4 MAC Layer Attacks. In Proceedings of the International Symposium on Wireless Personal Media Communications, 2007.
[11] A.Perrig, R.Szewczyk, R.Wen, D.Culler, J.D.Tygar, Spins: Security protocols for sensor networks. In Wireless Networks, 189–199, 2001.
[12] E.Luis, J.Palafox, Antonio Garcia-Macias, Security in Wireless Sensor Networks, 2008.