# Security Challenges in Wireless Networks

Swapnil S. Tale, Paras A. Tolia

Department of Computer Engineering, Sinhgad College of Enginnering,
Pune University, Vadgaon(Bk), Pune-411041

## ABSTRACT

Wireless networks have recently gained a lot of attention from the research community. Wireless Mesh Network (WMN) and Wireless Sensor Network (WSN) are characterized as multi-hop wireless networks. WMN is an integrated broadband wireless network which provides high bandwidth internet service to user; whereas WSN is an application oriented and generally set up for gathering records from insecure environments

Security has been a long trade off with Wi-Fi. Early wireless networks heavily leaned on WMNs to provide Layer 3 security, which kept aside from the additional overhead of encapsulation and challenges of roaming, Quality of Service, client support and scalability and left the IP network vulnerable to attacks. In the deployment of sensor nodes in an insecure 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.

There are several limitations and vulnerable features of WMN and WSN, along with the associated security threats and possible defenses. Security requirements for wireless networks are confidentiality, data integrity, data authentication and service availability.

**Keywords— WMN, WSN,** multi-hop wireless networks, Security requirements, sensor nodes**.**

## 1. INTRODUCTION

Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

A wireless sensor network (WSN) is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work[1].

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability. One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters[2].

## 2. OVERVIEW OF SECURITY ISSUES IN WIRELESS NETWORKS

### *A. Several Attacks and Threats*

Wireless Sensor networks are vulnerable to security attacks due to its broadcast nature of the transmission medium so many times it faces security problems. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in an environment where they are not physically protected[3]. An attack can be an effort to get illegal access to a service, information, or the check to conciliation integrity, confidentiality, or availability of a system. Attacks are attempted by adversaries [4]. Various kinds of attacks are:

- Active: Adversaries tries to add, delete or alter the packets on the ongoing transmission which threatens to confidentiality, authentication and data integrity.
- Passive: Adversaries or malicious node that only monitors the communication channel which threatens the confidentiality of data.
- Insider: Steal key material and run malicious code by compromise some authorized nodes of the network.
- Outsider: Attacker has no particular access to the network, it just keep the information about the ongoing transmission.
- Mote-Class Attacker: Has access to the minority nodes with similar capabilities.
- Laptop-Class Attackers: Attackers have access to powerful devices such as laptop which has advantages greater than legal nodes, for instance more capable processor, greater battery power and high power antenna.

### *B. Security Ethics*

The security requirements of a wireless sensor network can be classified as follows[4]:

- Data Authentication: Make sure that the data is initiated from the exact source.
- Data Confidentiality: Make sure that only authorized sensor nodes can get the content of the messages.
- Data Integrity: Make sure that any received message has not been modified in send by unauthorized parties.
- Availability: Make sure that services offered by WSN or by a single node must be available whenever necessary.

## 3. VULNERABILITIES IN WIRELESS NETWORKS

WMN and WSN are both multi-hop infrastructure-based wireless networks; however both have significant different purposes and objectives. WMN perform three levels of operations for internet provision to the end users, i.e. the

gateways form the top-levels and are connected with the wired network infrastructure for internet access. The middle levels constitute the mesh routers which form the multi-hop structure for providing access to the end-users. End-users mesh nodes form the lowest level. There are two types of mesh nodes present in WMN, one type of mesh nodes are directly connected with the mesh routers if they are in the direct communication range of mesh routers, if some nodes are not in the direct communication range of mesh routers, then WMN support the ad-hoc connectivity amongst the mesh nodes, i.e. the mesh nodes can connect with the wireless network trough other mesh nodes.

WSN operates in the same level where the WMN operates, i.e. there are no particular routers or gateways in the WSN; however all the nodes communicate with each other, they having router's capabilities for relaying data for each other. Some of sensor nodes may perform the gateways functionalities and all the nodes send the collected data towards the sink through the gateways node. Sink is a storehouse, which keeps all the collected data and figures to scientifically predict the outcomes of the network[5].

Although, the physical setup, topologies, operations and routing mechanisms are different in WMN and WSN, but yet both posses some common vulnerable characteristics and security challenges which may compromise the authentication, confidentiality, data integrity and service availability, etc.

### *A. Wireless Medium*

Jamming and scrambling are common security threats for the wireless medium of WSN and WMN. In jamming, the attacker uses a specialized hardware device to introduce a strong noise so that to create serious interference in the communication channels. Scrambling is periodical short term jamming in which the strong noise is introduces after specified interval of time, hence the communication channels of wireless medium work for some time and stop working during the period of scrambling it creates serious interferences in the ongoing transmission.

As a whole jamming and scrambling is used as a weapon against the wireless network's security especially in WMN and WSN, it can be used for jamming:

- Mesh nodes to detach them from network services and resources,
- Mesh routers to detach a portion of network,
- Mesh gateways to completely bring down the broadband services and resources,
- Sensor nodes to detach them from the rest of the network,
- Sensor gateways to stop the traffic flows toward the sink.

### *B. Cooperative MAC*

Both WMN and WSN use cooperative MAC (Medium Access Control) protocol at data link layer, which is shared amongst all the nodes in communication. Due to this cooperative MAC, hidden node terminal and collusion of packets problem occurs. The nodes can flood the packets of RTS(Ready to Send) toward the target node, as a result the target node will reply to each of the RTS with CTS(Clear to Send), hence creating extra overheads on the bandwidth, computation processing and power consumption. The malicious node can capture the MAC channel for indefinite period and continuous transmission; hence other nodes are unable to participate in the communication process. The cooperative MAC and the RTS/CTS mechanisms can seriously degrade the performance of WSN as compared to WMN.

### *C. Multi-hop environment*

WMN and WSN are multi-hop wireless networks. Data traffic passes in hop by hop pattern towards the destination. Multi-hop architecture is necessary for easy and rapid deployment, as well as it also reduce the deployment cost, as the nodes have the flexibility of self-healing, self-configuring and self-adjusting. This feature also greatly increase the reliability, as there exist many paths between the source and destination, and in case of any path failure, there exists alternate paths between source and destination to carry out the communication. On the other heads, this feature also has three negative aspects:

- Routing overheads increases
- Security risks increases
- Bandwidth decreases.

The main security threats due to the multi-hop nature of WMN and WSN are:

- Blackhole attack in which the malicious node drops all the traffic in the ongoing transmission.
- Greyhole attack, in which the malicious nodes selectively drop the network traffic in the communication channel.
- Wormhole attack, in which two distant malicious nodes forms a fast communication link, capture the packets at one end, forward it to the other through the fast link, and replayed the packets there to create routing disruption.
- False route creation attack, in which malicious nodes create false and non-existing routes between source and destination.
- Sybil attack, in which a malicious nodes shows many identities at a time, so create routing loops.

### *D. Power limitations*

As WSN consist of tiny nodes, which have limited or definite battery power. The sensor nodes conserve the energy by going to sleep-mode when there is no data to transmit over the network. The energy consume when sensor nodes transmit the data. In WMN, the mesh nodes may be static or mobile. Generally static nodes have no power limitations; however the mobile mesh nodes have power constraints.

The attackers can seriously degrade the performance of WSN, if strategically important nodes are under sleep-deprivation attack . The WSN has serious concerns regarding power limitations as compared to WMN nodes. As WMN support both static and mobile nodes, here the mobile nodes have limited supply and life of battery, however, if any mobile node of WMN is under sleep deprivation attack, it is of less severity and consequences limited to the mobile node only, i.e. the network operations remain unaffected.

## 4. LAYER WISE ATTACK

### *A. Physical Layer*

Jamming is a well-known attack on physical layer of wireless network. Jamming interferes with the radio frequencies being used by the nodes of a network. Jamming can interrupt the network impressive if a single frequency is used throughout the network. In addition jamming can cause excessive energy consumption at a node by injecting impertinent packets. The receiver's nodes will as well consume energy by getting those packets. Xu, Trappe, Zhang and Wood in 2005 proposed four different type of jamming attack that can be used by an attacker to stop the operation of

a wireless network. How each model affects on the sending and receiving capability of a wireless node and its impressiveness were evaluated. There are four possible threats in physical layer likewise: Interference, Jamming, Sybil and Tampering [4].

### *B. Data Link Layer*

Attacks can also be made on the data link layer. An attacker may premeditatedly violate the communication protocol, and frequently send messages in an attempt to cause collisions in the communication channel. This type of collisions would need the retransmission of any packet influenced by the collision. By means of this technique it would be possible for an adversary to consume easily a sensor node's power supply by forcing oversupply retransmissions. There are seven possible threats in data link layer likewise: Collision, Exhaustion, Spoofing, Sybil, De-synchronization, Traffic Analysis and Eavesdropping [4].

### *C. Network Layer*

A sensor node may get obtain benefit of multi hop using simply refusing to route messages at the network layer. This could be executed frequently or irregularly with the net result being that any neighbor who marks a route through the malevolent node at least will be incapable of exchange messages with, part of the network. Entry by force or without permission in network layer can be grouped into two categories of attacks: passive and active attacks. A passive trespass does not interrupt the functioning of the network; but the adversary to discover information, eavesdrops on the traffic flowing across the network without modifying the data. Passive attack does not take part in the ongoing transmission but it just keep track of information about the transmission and the data. It is very difficult to detect passive attack in view of the fact that a passive attack does not influence the functioning of the network. An active attack drops or modifies message thereby interfering the functioning of the network where both data packets and routing control packets kept by Messages. An attacker can attack routing packets causing a useless routing table at the source and these useless routing packets consumes energy of the nodes. So due to these whole network gets disturb and creates routing disruption [4].

On the other side, an attacker can attack data packets causing imperfect communication, although it assists with other nodes to make legal routes between senders and receivers, and causing routing disruption. For instance Wormhole attacks, Black hole attacks, Byzantine attacks, DoS attacks and routing attacks are counted as the active attacks.

### *D. Transport Layer*

Furthermore the transport layer is vulnerable to attack, as in the case of flooding. Flooding can be something simple such as sending many connection requests to a vulnerable node. In this situation, sender must be allocated to manage the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless [4].

## 5. SECURITY STANDARDS IN WIRELESS NETWORK

### *A. EAP: Extensible Authentication Protocol*

IEEE 802.11X provides an authentication framework that employs extensible authentication protocol (EAP) to support various authentication methods. EAP is a protocol that defines how to carry out authentication, but it is the EAP methods such as TLS, PEAP, LEAP, TTLS, and so forth that actually determine the answer to the question, are you really who you say you are? in the network authentication process. Being a point to point protocol (PPP), EAP authentication is based on the challenge/response communication paradigm. By postponing the authentication method at the link control phase, until the authentication phase, the EAP allows the authenticator/access point to request more information before determining the specific authentication method. The EAP authentication process can be summarized as:

- Requests, which indicate what is being requested, are sent from authenticator to requester.
- Type fields of the request and respond messages must match otherwise EAP authentication process must discard the packets. Authentication phase is completed with a success or failure message at the completion of the transmission [6].

### *B. WEP: Wired Equivalent Privacy Protocol*

WEP is the first solution suggested by the security standard; its objective is to make a WLAN equivalent to a traditional wired network and to ensure these 3 security services:

- Access Control, mechanisms and vulnerabilities: WEP has two types of authentication: open and shared key; the first does not offer any access security, the second is vulnerable, because it is enough to listen to challenge and answer to be able to access in a authorized way.
- Data Integrity, mechanisms and vulnerabilities: The integrity control is ensured by a CRC-32 algorithm. This mechanism having cons like linearity and non-complexity. The exploitation of these problems results in easy redirection attacks, as well as message injection.
- Data Confidentiality, mechanisms and vulnerabilities: WEP confidentiality is based on RC4 encryption algorithm, using 40 bits static keys + 24 bits initialization vectors sent in clear [7].

### *C. WEP2: Wired Equivalent Privacy version 2 Protocol*

WEP2 is an improved version of WEP, with increased initialization vector and key size, and with the use of 802.lx for periodical key change. However, WEP2 remains insufficient because the absence of protection mechanisms against collision, the use of RC4, etc [7].

### *D. WPA: Wi-Fi Protected Access Protocol*

To mitigate these insufficiencies in security, WiFi alliance agreed to use an intermediate solution called WPA**.** The latter takes parts of 802.1 li specification, where we have key management, Encryption with Temporal Key Integrity Protocol (TKIP) and data integrity with MIC. However, it still remains the problem consisting of the use of RC4 algorithm on which TKIP is based [7].

### *E. WPA2: Wi-Fi Protected Access version 2 Protocol*

WPA2 (or IEEE 802.11i-2004) in addition to TKIP, supports the AES-CCMP encryption protocol. Based on the very secure AES national standard cipher combined with sophisticated cryptographic techniques, AES-CCMP was especially designed for wireless networks. AES-CCMP requires more computing power compare to TKIP. Like WPA, WPA2 supports two modes of security, Personal and Enterprise [8].

## 6. CONCLUSION

Wireless Networks having few common limitations and challenges. Quality of Service, energy limitations, power limitation, security and multitasking are various challenges in Wireless Networks. The security of any wireless network should be checked frequently to detect attacks if any by the adversaries nodes and should be defensive to deploy new security mechanism. There are several security standards should be used as per the confidentiality concerns. Security methods provided by EAP to support a variety of upper layer authentication methods each with different benefits and drawbacks. Any one of these authentication methods can be the ideal choice for a specific networking environment and security requirements.

## 7. REFERENCES

[1] John A. Stankovic, "Wireless Sensor Networks", www.wsntech.net (2006).

[2] SANS Institute InfoSec Reading Room, "Wireless LAN: Security Issues and Solutions"(2003).

[3] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security,(2009).

[4] H. Modares, R, Salleh, A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence,(2011).

[5] 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,(2009).

[6] Khidir M. Ali, Ali Al-Khalifah, "A Comparative Study of Authentication Methods for Wi-Fi Networks", A Comparative Study of Authentication Methods for Wi-Fi Networks,(2011).

[7] N. CHENDEB, B. E. HASSAN, and H. AFIFI, "Performance evaluation of the security in wireless local area networks (WiFi)", International Conference on Information and Communication Technologies,(2004).

[8] I. P. Mavridis, A. B. Halkias, "Real-life paradigms of wireless network security attacks", Panhellenic Conference on Informatics,(2011).