Survey of Current and Future Trends in Security in Wireless Networks

Vikas Solomon Abel

Abstract— Security has always been a key issue with all the wireless networks since they have no physical boundaries. Many existing and evolving threats which must be considered to ensure the countermeasures are able to meet the security requirements of the environments for which it is expected to be deployed.

Index Terms— Bluetooth, Wi-Fi, WiMax, Wireless Sensors, WLAN

1 Wireless Technologies

Wireless Broadband is a fairly new technology that provides high-speed wireless internet and data network access over a wide area. The three most important broadband wireless technologies are IEEE 802.11, IEEE 802.16, and Wireless Mesh Network (WMN). In Wireless Broadband Networks Privacy and Integrity of data are key considerations for both broadband networks. Authentication and Security to prevent unwanted access to critical data or services are necessary for the effective operation of any broadband network. The motivation behind Wireless Broadband technology was the support of mobile clients within a certain range and to provide wireless network infrastructure in such places where wired networks are not feasible or possible.

WLAN which is IEEE 802.11 technology consist of two important components, i.e. nodes and an Access Point (AP). The AP provides wireless connectivity to nodes as well as function as a bridge between the nodes and wired network infrastructure. Probe request frames are used by the clients to discover a wireless network. If a wireless network exist then the AP respond with Probe response frame. The AP (Access Point) which provides the strongest signal is selected. If the AP is overloaded then the nodes connect with another nearby AP although the signal strength is relatively weak [1]. Typical applications of WLAN are campus and organizational networking; back haul for public safety and industrial control networks [2]. WLAN may be an Infrastructure WLAN where client devices communicate wirelessly to a wired Local Area Network (LAN) such as Ethernet, via Access Points or an Ad-Hoc WLAN in which devices or stations communicate directly with each other, without using Access Points or a connection to the wired network. For wireless devices in a WLAN to communicate with each other, they must all be configured with the same SSID. Wireless devices have a default SSID that is set at the factory. Some wireless devices refer to the SSID as network name.

Wi-Fi or Wireless Fidelity is to connect to the internet at high speeds. Wi-Fi enabled devices operates in unlicensed spectrum. They use radio technologies within the range of an access point for data communication which are based on the IEEE 802.11 standards. The benefits of using Wi-Fi in the last mile are that, the client device is so cheap due to large volume of production [3].

Sensor networks often have one or more points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. They may also be referred to as sinks. Base stations are typically more powerful than sensor nodes. Sensors are constrained to use lower-power, lower-bandwidth, shorter-range radios. Sensor nodes form a multihop wireless network to allow sensors to communicate to the nearest base station.

Aggregation points help in reducing the total number of messages sent thus saving energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points. An aggregation point may collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. It is also possible that every node in the network functions as an aggregation point, delaying transmission of an outgoing message until a sufficient number of incoming messages have been received and aggregated. Power management in sensor networks is vital [4].

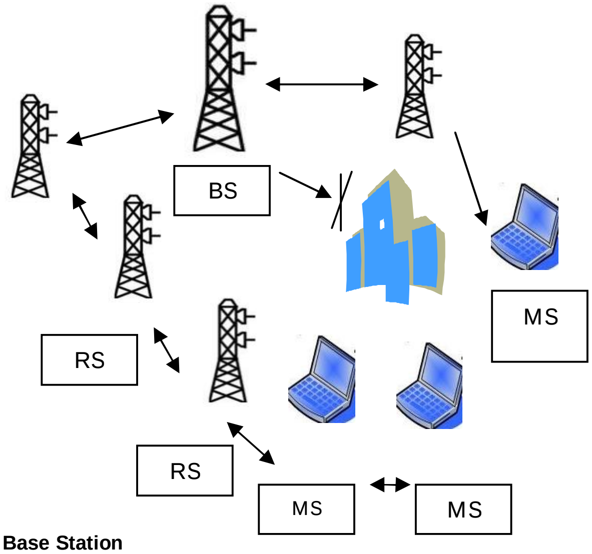
WMN is an emerging broadband wireless technology which consists of mesh routers and mesh nodes. The mesh routers form the backbone and provide connectivity to mesh nodes. With some of the mesh routers in WMN the functionality of gateways is provided for internet connectivity to mesh nodes. The WMN nodes act both as a client and as a relay router for forwarding traffic for other nodes. In most of the cases, the WMN form partial mesh topology, which means that there are many routes to every node, so if any route is not working then the data traffic can be sent through other route [2].

Bluetooth is a universal radio interface in the 2.45 GHz frequency band that enables portable electronic devices to connect and communicate wirelessly via short-range, ad hoc networks. Each unit can simultaneously communicate with up to seven other units per piconet. Moreover, each unit can simultaneously belong to several piconets [5].

Bluetooth uses a radio technology called frequency-hopping spread spectrum. A Bluetooth device will use many different and randomly chosen frequencies every second to minimize the probability of other devices using the same frequency and to minimize interference time. For battery operated devices Bluetooth is ideal. It does not rely on the user input since it can automatically detect and communicate with other Bluetooth devices. The frequency of Bluetooth capable devices ranges from 2.402 GHz to as high as 2.480 GHz, a frequency range specifically reserved by international agreement for ISM or medical, industrial and scientific devices.

WiMAX, an acronym for Worldwide Interoperability for Microwave Access, is a telecommunications technology that provides fixed and fully mobile internet access. The IEEE 802.16 standard forms the basis of . Clarification of the formal names are as follow:

802.16-2004 is also known as 802.16d, which refers to the working party that has developed that standard. Since it has no support for mobility it is sometimes referred to as "Fixed WiMAX". 802.16e-2005, is also known as 802.16e, is an amendment to 802.16-2004. It introduced support for mobility, among other things and is therefore also known as "Mobile WiMAX". 802.16j-2009, the Multihop Relay specification for 802.16.



BS – Base Station
RS – Relay Station MS – Mobile Station

Fig 1. Multi-hop Relay Network architectures
Source : [23]

2 General Attacks on Wireless Networks

General, attacks on wireless networks may be divided into four basic categories: passive attacks, active attacks, man-in-the middle attacks, and jamming attacks.

A passive attack occurs when someone listens to or eavesdrops on network traffic. A passive attack on a wireless network may not necessarily be malicious in nature. They are very difficult to detect.

In passive attacks the attacker is not concerned with the routing protocol. It only eavesdrops on the routing traffic and endeavours to get valuable information like node hierarchy and network topology from it. For example, if a route to a particular node is requested more than other nodes, the attacker might predict that the node is important for the operation of the network, and putting it out could bring down the entire network. Even when it is not possible to isolate the precise position of a node, one may be able to determine information about the network topology by analysing the contents of routing packets. This attack is very difficult to detect and prevent [6].

In active attacks, the aggressor node has to spend some of its energy in order to carry out the attack. Nodes that perform active attacks with the aim of disrupting other nodes by causing network outage are considered to be harmful, while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. The harmful or malicious nodes can change the routing information by modifying, fabricating or impersonating nodes and thereby disrupting the correct functioning of a routing protocol [6].

Once an attacker has gained enough information from the passive attack, the hacker can then launch an active attack against the network. There are an large number of active attacks that a hacker can launch against a wireless network. Some examples of the attacks are Spoofing attacks, Unauthorized access, Flooding attacks etc. Spoofing occurs when a malicious node misrepresents its identity by altering its MAC or IP address in order to mislead the information about the network topology. It can also create routing loops etc.

3 General Physical layer Attacks

3.1 Jamming Attacks on Wireless Networks

Jamming is a attack specific to wireless networks. Jamming occurs when spurious RF frequencies interfere with the operation of the wireless network. In some cases, the jamming may be unintentional and is caused by the presence of other devices such as cordless phones, that operate in the same frequency as the wireless network. Intentional and malicious jamming occurs when an attacker analyzes the spectrum being used by wireless networks and then transmits a powerful signal to interfere with communication on the frequencies discovered.

3.2 Scrambling

Scrambling is a type of jamming attack for short intervals to disorder targeted frames (mostly management messages) which ultimately lead to network failure.

3.3 Water Torture Attack

In this attack the attacker pushes a Subscriber Station (SS) to drain its battery or consume computing resources by sending bogus frames [7].

3.4 Man in the Middle Attack

In this attack an attacker intercepts the valid frames and then intentionally resends the frames to the target system. A wireless – specific variation of man-in-the-middle attack is placing a rogue access point within range of wireless stations. If the attacker knows the SSID in use by the network, he can gain information such as the key information, authentication requests and so on. It may involve spoofing an IP address, changing a MAC address to emulate another host, or some other type of modification.

3.5 Denial of Service Attack

In a "denial-of-service" attack an attacker may try to prevent an authentic user from using a service. This may be done by "flooding" a network, disrupt connections between two machines etc. The common method is to flood a network with degenerate or faulty packets and hence denying access to the legitimate traffic.

3.6 Physical Tampering

In this attack the physical device may be tampered and sensitive information can be extracted from it.

4 General Link layer Attacks

4.1 Unencrypted Management Communication

Almost all the IEEE 802.16 management messages are still sent unencrypted. The IEEE 802.16-2004 standard does not provide any capability to encrypt management messages.

4.2 Masquerading threat

By intercepting the management messages an attacker can use the hardware address of another registered device. Once this is successful an attacker can turn a Base Station (BS) into a Rogue Base Station [7]. A rouge WiMAX base station pretends to be a valid base station, and then drops/eliminates all/some of the packets.

4.3 Threat due to Initial Network Entry

In IEEE 802.16j-2009 no integrity protection for management messages can be made in case of multicast transmissions and in case of initial network entry by a new candidate node [8].

5 General Network layer Attacks

The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. Routing messages in Ad Hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Data packets are forwarded by intermediate nodes along an established route to the destination based on the routing states. Both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. Network-layer vulnerabilities generally fall into one of two categories: routing attacks and packet forwarding attacks, based on the target operation of the attacks [9].

In the context of DSR [11], the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list [12]. In AODV [10] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [13]. By attacking the routing protocols, the attackers can pull traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not the optimal route or which may even be nonexistent. The attackers can also create routing loops in the network [9].

Attacks may be launched in addition to routing attacks such as in packet forwarding operations. These attacks do not disrupt the routing protocol but poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. The attacker may drop or modify the contents of the packets or duplicate the packets it has already forwarded. Attacker may also inject large amount of bogus packets into the network which wastes a significant portion of the network resources and introduces severe wireless channel contention and network congestion in the MANET [9].

Routing protocols for ad-hoc networks are based on the assumption that intermediate nodes do not maliciously change the protocol fields of messages passed between nodes. This assumed trust permits malicious nodes to easily generate traffic subversion and denial of service (DoS) attacks. Attacks using modification are generally targeted against the integrity of routing computations and so by modifying routing information an attacker can cause network traffic to be dropped, redirected to a different destination, or take a longer route to the destination increasing communication delays. Forged routing packets may be sent to other nodes to divert traffic to the attacker or to some other node. The intention is to create a black hole by routing all packets to the attacker and then discarding it. As an extension to the black hole, an attacker could build a grey hole, in which it intentionally drops some packets but not others, for example, forwarding routing packets but not data packets. A more subtle type of modification attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private network connection [6]. A brief description of the attacks is as follows -

5.1 Blackhole Attack

In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), hiding from the source the information that the data did not reach its intended recipient. The black holes themselves are invisible, and can only be detected by monitoring the lost traffic. An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets [14].

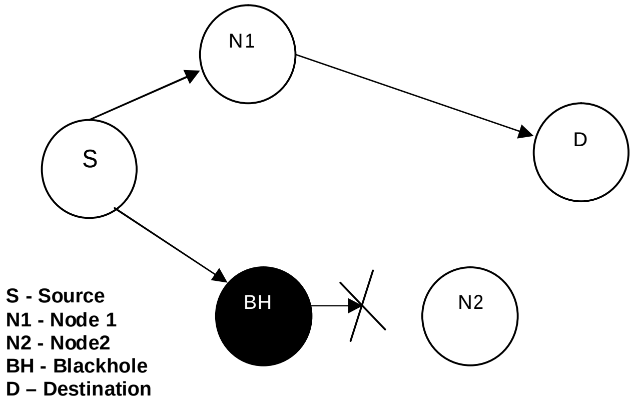


Fig 2. Blackhole Attack
Source : [22]

The properties of Blackhole attack is that firstly, the Blackhole node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is false, with the intention of intercepting packets. Secondly, the packets are consumed by the Blackhole node. Thirdly, the Blackhole nodes can conduct coordinated attacks.

5.2 Greyhole Attack

Grey Hole is a node that can change from behaving correctly to behaving like a black hole so as to avoid detection. Some researchers discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to a Route Reply (RREP) only allowing the destination to reply [15].

5.3 Wormhole Attack

In a wormhole attack, an attacker forwards packets through a out-of-band high quality link and replays those packets at another location in the network [16].

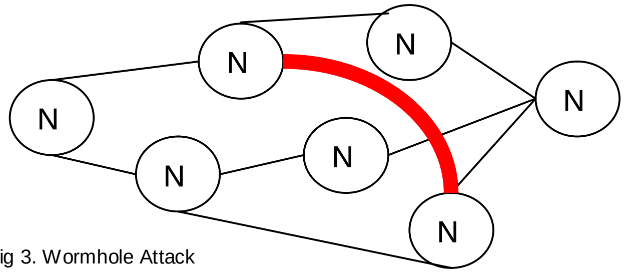


Fig 3. Wormhole Attack

Wormhole attacks depend on a node misrepresenting its location. Hence, location based routing protocols have the potential to prevent wormhole attacks .

5.4 Flooding Attack

In a flooding attack, the attacker targets the target node by flooding in order to congest the network and degrade its performance [17].

5.5 Rushing Attack

In Multicast forwarding a single stream of data is sent to multiple receivers so as to save network bandwidth. A rushing attacker exploits duplicate suppression mechanism by quickly forwarding route discovery packets and hence gaining access to the forwarding group. The goal of this attack is to invade into routing paths. The Multicast routing protocols are targeted which reduce routing overheads. The method is to quickly forward route discovery (control) packets by skipping processing or routing steps [18].

5.6 Jellyfish Attack

In a jellyfish attack the attacker first needs to intrude into the multicast forwarding group. Then data packets forwarding are delayed for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real applications. It causes a increase in end –end delay [18].

5.7 Sybil Attack

In a Sybil attack a large numbers of shadow identities are generated and controlled by the malicious parties. Each radio represents a single individual. However the broadcast nature of radio allows a single node to pretend to be many nodes simultaneously by using many different addresses while transmitting [18].

6 Transport Layer Attacks

Transport layer attacks may occur during authentication and securing end-to-end communications which can be rectified through data encryption [9].

The transport layer is responsible for managing end-to-end connections. Two possible attacks in this layer, flooding and desynchronization as in case of sensor networks .

6.1 Flooding

By repeatedly make new connection requests until the resources required by each connection may be exhausted, may reach a maximum limit or may lead to memory exhaustion through flooding. In either case, further legitimate requests will be ignored. One proposed solution to this problem is to require that each connecting client demonstrate its commitment to the connection via the solving of a puzzle. The idea is that a connecting client will not needlessly waste its resources creating unnecessary connections. Since an attacker does not likely have infinite resources, it will be impossible for them to create new connections fast enough to cause resource starvation on the serving node. Although these puzzles do include processing overhead, this technique is still more desirable than excessive communication [20].

6.2 Desynchronization

Disruption of an existing connection is refered to as Desynchronization [19]. An attacker may, for example, repeatedly spoof messages to an end host causing that host to request the retransmission of missed frames. This degrades the ability of the end hosts to successfully send and receive data.

7 Session Layer Attacks

In Session Layer attack an attacker attempts to hijack an established TCP session between two computers by guessing the sequence numbers and taking out one of the user. The counterattacks can be using encryption techniques, limiting incoming traffic etc.

8 Application layer Attacks

Application Layer attacks involve viruses, worms, malicious codes, application abuses etc [9]. When data being transmitted is unencrypted, it is vulnerable to sniffing as well as attacks against applications. Several additional features must be implemented within network equipment to ensure against sniffing of data packets as shown in the figure to provide additional security [21].

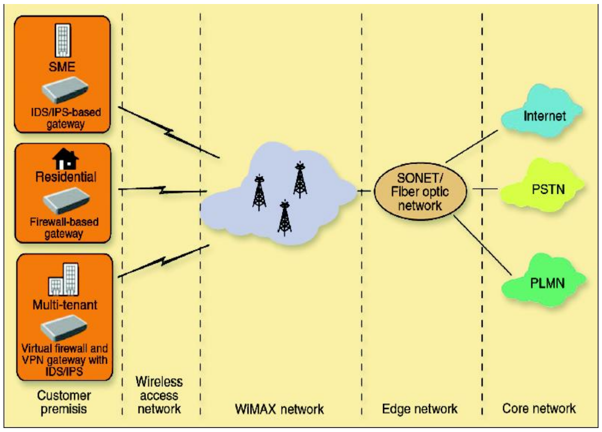


Fig 4. A typical security infrastructure
Source : [21]

9 Future Work

Future work involves the study of the Identity attacks in Wireless networks. Experimental studies will be conducted in different Wireless Technologies studying the effect of Identity attacks in different scenarios. Possible techniques to identify and counterattack such attacks will be suggested.

References

[1] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose and D. Towsley, “Facilitating Access Point selection in IEEE 802.11 wireless networks” , Proceedings of 5th ACM Conference on Internet Measurement, 2005.

[2] S. Khan, K.Loo, T. Naeem, M. Hhan, “ Denial of Service Attacks and Challenges in Broadband Wireless Networks ”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008.

[3] V. Gunasekaran, F. Harmantzis, “Emerging wireless technologies for developing countries ”, Technology in Society 29 23–42, 2009.

[4] C. Karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[5] J. Haartsen, “BLUETOOTH—“The universal radio interface for ad hoc, wireless connectivity” , Ericsson Review No. 3, 1998.

[6] A. Pirzada, C. McDonald, “Establishing trust in pure ad-hoc networks”, in: CRPIT ’04: Proceedings of the 27th Conference on Australasian Computer Science, Australian Computer Society Inc., Darlinghurst, Australia, 2004, pp. 47–54.

[7] H. Kim, Department of Electrical and Computer Engineering, Stevens Institute of Technology, “IEEE 802.16/WiMAX Security”, 2006.

[8] M. Bogdanoski, P. Latkoski, A. Risteski, Borislav Popovsk, “IEEE 802.16 Security Issues: A Survey”, 16th Telecommunication forum, TELFOR 2008.

[9] H Yang, H Luo, F Ye, S Lu, L Zhang , “Security in mobile ad hoc networks: challenges and solutions”, IEEE Wireless Communications, 2004 – Citeseer.

[10] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,”, *2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, 1999.

[11] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Mobile Computing*, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

[12] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks”, *ACM MOBICOM*, 2002.

[13] M. Zapata, and N. Asokan, “Securing Ad Hoc Routing Protocols,” *ACM WiSe*, 2002.

[14] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon ,K. Nygard , “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” , In Proceedings of the International Conference onWireless Networks, Las Vegas, June 2003.

[15] Ebrahim Mohammed Louis Dargin,Oakland University School of Computer Science and Engineering CSE 681 Information Security, “Routing Protocols Security in Ad Hoc Networks”, Citeseer.

[16] L. Hu, D. Evans, Department of Computer Science , University of Virginia Charlottesville, “ Using Directional Antennas to Prevent Wormhole Attacks”, *Network and Distributed System Security Symposium* (NDSS), February 2004.

[17] S. Khan, K.Loo, T. Naeem, M. Khan , “Denial of Service Attacks and Challenges in Broadband Wireless Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008.

[18] V. Palanisamy, P.Annadurai, “Impact of Rushing attack on Multicast in Mobile Ad Hoc Network” , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[19] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks”, *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[20] Y. Wang, G. Atterbury, B. Ramamurthy, “A survey of security issues in wireless sensor networks”, IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006.

[21] R. Mylavarapu, “Security considerations for WiMAX- based converged network”, http://rfdesign.com, August 2005.

[22] V. Abel, “Survey of Attacks on Mobile Adhoc Wireless Networks”, International Journal on Computer Science and Engineering, ISSN : 0975-3397, Vol. 3 No. 2, 2 Feb 2011.

[23] V. Abel, A. Mnaouer, “On the Study of the WiMAX Security Threats and Current Solution Trends”, Journal of the Caribbean Academy of Sciences, 2010.