Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks

Shafiullah Khan[*1,2], Noor Mast[*1,2], Kok-Keong Loo[*1], Ayesha Salahuddin[*3]
[*1]*School of Engineering and Design, Brunel University, UK*
[*2]*IIT Dept. Kohat University of Science and Technology (KUST), Pakistan*
[*3] *Allama Iqbal University Computer Science Department Islamabad, Pakistan*
{Shafiullah.khan, Noor.mast, Jonathan.loo } @brunel.ac.uk,
Ayesha_iiui@hotmail.com

Abstract

The Wireless Mesh Network (WMN) is ubiquitous emerging broadband wireless network. However, the open wireless medium, multi-hop multi-radio architecture and ad-hoc connectivity amongst end-users are such characteristics which increases the vulnerabilities of WMN towards many passive and active attacks. A secure network ensures the confidentiality, integrity and availability of wireless network. Integrity and availability is compromised by active attacks, while the confidentiality of end-users traffic is compromised by passive attacks. Passive attacks are silent in nature and do not harm the network traffic or normal network operations, therefore very difficult to detect. However, passive attacks lay down a foundation for later launching an active attack. In this article, we discuss the vulnerable features and possible passive threats in WMN along with current security mechanisms as well as future research directions. This article will serve as a baseline guide for the passive security threats and related issues in WMNs.

Keyword

IEEE 802.11, Wireless Mesh Network, Security, Passive Attack, Active Attack, Broadband

1. Introduction

Today WMN are increasingly becoming the interests of researchers, end-users and industries. Researchers are interested as there are still unresolved challenges needed to be addressed before large scale exploitation takes place. End-users are interested as they need such a broadband technology which is secure, available everywhere anytime, and low cost. Industries are interested, as this can be the revolutionary integrated wireless technology, which is going to bring integration between the other wireless and wired networks, and is capable to generate huge revenue. WMN is a decentralized, low cost, easily deployable, self-healing and self-configuring wireless broadband network, and these characteristics make it superior than other wireless broadband technologies. Other broadband technologies such as IEEE 802.11, DSL, ISDN and IEEE 802.16 are difficult to deploy as they requires centralized controlling, managing, monitoring, and expensive maintenance and deployment cost.

Some features such as the multi-hop, multi-radio ad-hoc nature, dynamic mesh topological changes and the attack prone wireless medium access of WMNs are making it vulnerable to different security threats both active and passive attacks. A passive attack is the first step toward launching an active attack against the wireless broadband network like WMN. The severe impact of active attack is the unavailability of broadband services or network bandwidth. To minimize the possibility of launching an active attack, there is a need to address the first-step i.e. passive attacks related issues prior to the commercial deployment of WMN.

This article presents four principal findings. First, the important characteristics and different kinds of possible passive attacks are pointed out. Second, some vulnerable features of WMN are identified. Third, consequences of passive attacks in WMN are described. Finally, shortcomings of current security mechanisms for defending passive attacks are discussed and possible countermeasures are introduced. This article will serve as a baseline guide for the researchers to address passive security issues in WMN.

2. Threat-prone features of WMN

As an integrated wireless broadband technology, WMN not only provides internet services to end users but also integration amongst different wired and wireless networks. Three features of WMN are making it vulnerable to different security threats especially passive attacks.

- Large scale broadband wireless network
- Multi-hop architecture
- Ad hoc type connectivity amongst end-users devices

The architecture of WMN is depicted in Fig. 1. As a large scale broadband wireless network, WMN is very flexible and dynamic in providing internet services to end-users. End-users have the freedom to join or leave the network from anywhere anytime; hence it is difficult to detect active and passive attacks in such a vast broadband wireless network.

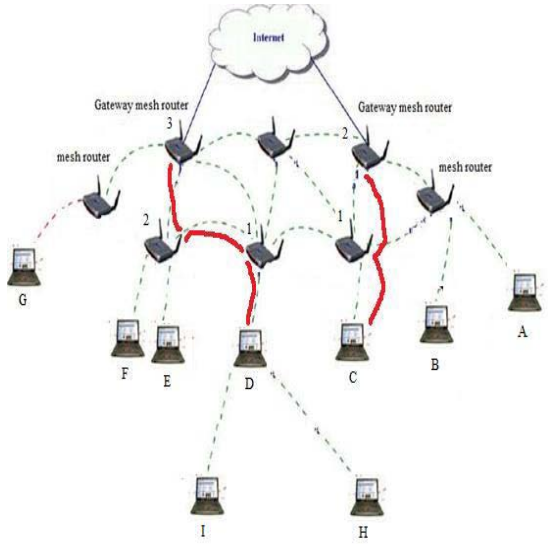

Figure 1. Typical architecture of WMN

Multi-hop structure is important for flexibility, easy deployment and to increase the coverage area of WMN, however vulnerable to most of the active and passive attacks. Increasing in number of hops creates three problems in WMN.

- Unfair bandwidth allocation. Bandwidth in WMN decreases with increasing number of hops as ½ of the total bandwidth at first hop, $1/4^{th}$ of the total bandwidth at 2^{nd} hop, and $1/8^{th}$ at 3^{rd} hop.
- More possibilities of active attacks.
- More chances of passive attacks.

The multi radio ad hoc type connectivity enables The end users to access the broadband services through another node, if it is not in the direct communication range of Access Point (AP) or wireless mesh router. As in WMN, the nodes can also function as a router to relay traffic for nearby nodes. However, this kind of connectivity can again result in active attacks as well as passive attacks. As shown in Fig. 1, node D can launch active attacks against node I and node H such as battery exhaustion attack by forwarding unnecessary traffic to them, or act as a blackhole by dropping all the traffic going toward them. Similarly, node D can launch passive attacks against node I and H.

3. Passive threats in WMN

In passive attacks, the attackers simply analyze and listen to the network traffic with the objective to capture sensitive information of the target. These kinds of attacks compromise the confidentiality of the end user traffic. In passive attack, the unauthorized user gain illegal access to the network traffic without modifying the traffic [5]. Passive attacks are very difficult to detect [2] as such attacks do not harm the user traffic or normal network operations. In passive attacks, the attacker measures the length, time and frequency of wireless transmission to get some valuable information.

3.1 Eavesdropping

Due to the characteristic of open wireless medium, the broadband wireless networks are easily victimized for eavesdropping as they use air as a medium for data transmission over wireless network connections. To eavesdrop such wireless connections are not difficult. WMN is more vulnerable to eavesdropping as compared to IEEE 802.11. As the IEEE 802.11 provides broadband services to an organization or limited group of users, so the attackers need to be close to the premises of an organization to eavesdrop the wireless link, while, WMN is a community based broadband wireless network which support large scale users, so the attackers can eavesdrop any desired wireless link easily. The eavesdropper can capture and listen to the on-going traffic of communication channels using such tools which are easily available. Eavesdropping can be successfully conducted with the help of sniffers. A sniffer may be an application or device which is able to read and capture the network packets. The sniffer applications can also be used to detect SSID and collect the MAC addresses of the nodes. This attack is less severe for the wireless network, however more severe for the target user, if sensitive information are captured such as credit card number, social security number. Strong encryption is the possible way to defend eavesdropping.

3.2 Traffic analysis

WMN is multi-hop wireless broadband technology,

and as the number of hops increases between the source and the destination, routing overheads and security risks increases. Traffic analysis [6] is a network based attack against WMN in which the network traffic is intercepted and examined to collect information for many reasons such as

- To locate the source and destination nodes.
- People in communication.
- Military intelligence.

WMN is more vulnerable to traffic analysis due to its multi-hop architecture as compared to IEEE 802.11 which is single-hop. As shown in Fig. 1, node C is two hops away from the broadband services, while node D is three hops away. In this case, node D is not only receiving less bandwidth, but also more vulnerable to traffic analysis kind of passive attacks as compared to node C. Similarly, node I and H are not in the direct communication range of any AP, therefore node D is acting as a router and relaying traffic for node I and H. Here, if node D is malicious, then it is in the perfect position to analyze all the in and out traffic of both I and H nodes. Traffic analysis can also be used for homing attack, in which the attacker analyzes the traffic pattern to locate the gateway [3]. The purpose of homing attack is to achieve DoS by jamming the gateway to create broadband unavailability.

Most of the routing protocols tested on WMNs are adapted from ad-hoc networks. In proactive ad hoc routing protocols, mobile nodes constantly exchange routing updates in which can easily be captured by adversary to get information about the entire topology and nodes location. On-demand routing protocols are less vulnerable to traffic analysis as the routes are established when needed. However the DSR is still vulnerable to passive traffic analysis as the route information are kept in packet headers, and if a single packet is captured by the adversary then the entire routes and forwarding nodes can be judged [1]. The defence mechanisms against this security threat can be:

- Multi-path routing, i.e. establishment of many routes between source and destination such that adversary will not be able to get all the information from a single path. However, multi-path routing may increase the routing overheads..
- Masking i.e. sending continuous encrypted signals even the traffic is not transmitted from source to destination.

3.3 Corrupt Access Point

In IEEE 802.11 WMN, the APs and the wireless mesh routers serve as the backbone devices, and nodes are connected with it for broadband access. In this attack, the attacker accesses the device without changing its configuration. Being a large scale wireless broadband network, WMN can easily be victimized for corrupt AP attack as compared to IEEE 802.11 Wi-Fi, as IEEE 802.11 has limited coverage for a single organization or target group of users, therefore the adversary needs to be closed to the target AP, while WMN is community based broadband wireless network which can provide broadband services to a whole city, therefore the adversary can launch such an attack on any nearby AP or wireless mesh router. Once the AP or wireless mesh router is compromised then the adversary is able to analyse the traffic of all the nodes passing through it. Such kind of attack is very difficult to detect. One solution to this kind of attack is the periodic erasure and reprogramming of the AP [4]. However this is not the perfect solution as during the reprogramming and erasure process, the end-users will not be able to access the network. The attacker usually uses brute-force approach to break the password of such an AP. This attack is more severe in nature, as the adversary is now able to monitor the network traffic of all the attached nodes. This attack can easily be converted to an active attack by dropping the packets or selectively forward the network traffic and even can result in a Denial of Service attack by disconnecting this portion from the WMN.

3.4 War-driving attack

WMN uses free radio frequency bands i.e. 2.4GHz. The radio frequency signal may not be confined or restricted to a specific area, so any potential attacker with a wireless device can gain access to the network, and use the network resources. The main objective of an organizational secure network is to “keep the outsider out” from accessing the organizational network resources [7]; such kind of attack is a real violation of an organization’s secure network policy. Furthermore, most of organizations use broadcast SSIDs and simple passwords, so in such case, the attacker can easily penetrate into the wireless network. Here if the objective of an attacker is just to use the network resources of an organization, then it is passive attack. But if the objective is to harm the network resources of an organization, then it will be an active attack. As earlier discussed, the objectives of most of the passive attacks are to conduct active attack later. Again due to the large coverage area of WMN, the adversary can conduct war-driving attack from anywhere.

3.5 Brute force attack

Most of the APs in the same wireless network use the same user names and passwords; once known, the attacker can get complete control of the network. If different passwords are used, then brute force attack is used to break the password of an AP or mesh router by periodically testing every possible password from brute force dictionary. APs having broadcast usernames and weak or static passwords can easily be compromised [18]. If the brute force attack is only used for traffic analysis then it is passive attack otherwise active.

After any successful passive attack, the adversary has the desired information about the target node/nodes and is able to conduct an active attack which would be of worse consequences if the target node is the gateway.

4. Consequences of passive attacks in WMN

Table 1. Passive attacks with possible defences

Characteristics	Passive attack	Can result in Active attack	Defences
Multi-hop	Homing	DoS, Jamming, Flooding	Header Encryption
	Traffic Analysis	Blackhole, Greyhole, Wormhole, Rushing,	Secure routing protocol hop-by-hop encryption multi-paths routing
	Corrupt AP	DoS, routing Disruption, Network partition,	Authentication and authorization
Open Wireless medium and Ad-hoc connectivity	War Driving	Flooding or Distributive flooding on AP	Strong authentication, MAC filtering
	Brute force	DoS (AP),	Strong authentication, periodically change the password
	Eaves-dropping	Jamming, MAC selfishness, Battery exhaustion RTS/CTS exploitation	Strong Encryption Trust management mechanism between nodes Digital signature Authentication

Table 1 summarises the potential passive attacks in WMN and the possible defence mechanisms. Passive attacks provide a ground for later launching active attacks or launching more severe active attack like DoS. For example, an attacker get illegal access to wireless AP or wireless mesh router using sniffers or using brute-force mechanism and passively monitoring the ongoing traffic of all the attached nodes. The attacker can select a target node for active attacks by selectively or fully dropping and/or modifying its packets keeping it isolate from performing normal network operations, and can result in more severe attack if the attacker decides to harm the AP or mesh router by isolating that portion of wireless network.

5. Security mechanisms and possible future directions

Confidentiality can be maintained with the help of strong encryption and authentication mechanisms. IEEE 802.11 WMN uses the following mechanisms for this purpose.

- Wired Equivalent Privacy (WEP)
- WEP1
- Wi-Fi Protected Access (WPA1)
- WPA2

WEP is implemented in the MAC layer. The shared secret keys of WEP are almost static, i.e. remains the same even for years. This provides enough time to hackers to analyze and hack into WEP enabled wireless networks. In light, WAP1 which uses a 64-bit encryption (40-bit encryption key and 24-bit initialization vector) for both client and AP [10] which can easily be compromised by the adversary, and it can easily be broken by mean of Brute Force attack [9]. Furthermore as the Initialization Vector (IV) is small and sent as a plaintext, this may result in IV key reuse attack. WEP2 is an updated version of WEP, which uses 128-bit initialization vector; however it also suffers from the same kind of vulnerabilities as observed in original WEP.

Table 2. Characteristics of WEP and WPA

Characteristics	WEP	WPA
Encryption method	RC4	RC4, TKIP
Key size	40-bits	128, 192, 256-bits
Hash method	ICV	ICV, Michael
Authentication	Optional	Required
Key distribution	Manual	TKIP
Vulnerabilities	Key reuse attack, weak encryption.	Birthday attack, Differential cryptanalytic attack, DoS,

WPA provides encryption via the Temporary Key Integrity Protocol (TKIP) and addresses the weaknesses of WEP by providing enhancements such as Per-Packet key construction and distribution, a message integrity code feature and a stronger IV. However, it needs firmware upgrade of the current hardware, and one may have to get a new hardware to take the advantages of

this encryption mechanism. The length of a WPA key is between 8 and 63 characters i.e. the longer it is the more secure it is [9]. WPA is also vulnerable to 60-seconds DoS attack, if the AP detects unauthorized data [8].

WPA2 uses more powerful method of encryption, Advanced Encryption Standard (AES). AES supports key sizes of 128 bits, 192 bits, and 256 bits. It is backward compatible with WPA and uses a fresh set of keys for every session. The characteristics of WEP and WPA are summarized in Table 2.Keeping in view the above limitations of existing encryption and authentication mechanisms, we need enhanced security systems for the multi-hop ad-hoc broadband WMN. To deal with passive attacks and to protect the confidentiality, security mechanisms needs to be investigated are given in Table 1, and are summarize below.

The utmost priority for the research community is to protect this multi-hop broadband wireless network from security attacks, in particularly passive attacks because they are the starting point for most of the active attacks.

- Secure routing protocol which is capable of hop-by-hop encryption so that to defend most of the active and passive attacks caused by multi-hop architecture of WMN.
- Trust management and strong authentication mechanisms are required to avoid the security threats raised by the ad-hoc type connectivity amongst mesh nodes.
- Spread spectrum techniques and enhanced encryption mechanisms are desirable to handle the security risks enforced by the open wireless medium of WMN.

6. Conclusions

The broadband nature, multi-hop architecture, multi-radio interface and dynamic ad hoc meshed topology are such characteristics of WMN due to which it is more vulnerable to different security attacks both active and passive. Active attacks compromise the date integrity and service availability of WMN while passive attacks violate and compromise the confidentiality and secrecy of nodes and traffic of end users. The passive attacks lay a foundation for later launching an active attacks either against the wireless network resources or end-users nodes. Thus it is necessary to address such security issues before the commercial deployment. So far, many security mechanisms exist but they are unable to protect the confidentiality and privacy of end-users. Our finding suggests that to combat passive threats and to protect the confidentiality, some improved mechanisms are required for the three vulnerable features of WMN such as secure routing protocol and hop-by-hop encryption to address the multi-hop related attacks, trust management and authentication mechanisms amongst the end users to overcome the ad-hoc connectivity challenges, and enhanced spreading and encryption mechanisms at physical layer and link layers.

However, any security mechanism, which is proposed to address the passive threats in WMN must not create other problems such as increase routing overheads, slowdown communication, consume more bandwidth, create jitter or reduce throughput. Only a secure and fast WMN will be highly accepted for commercial deployment as a popular wireless low cost broadband technology.

7. References

[1] J. Kong, X. Hong, M. Gerla, “A new set of passive routing attacks in mobile ad hoc networks,” IEEE Military Communication Conference (MILCOM), 2003.

[2] R.C. Phan, “Security limitations of an authorized anonymous ID-base scheme for mobile communication,” IEEE Communication Magazine, May 2005.

[3] D.R. Raymond, S.F. Midkiff, “Denial-of-Service in wireless sensor networks: attacks and defences,” IEEE Security and Privacy, pp. 74-81, 2008.

[4] N.B. Salem, J.-P Hubaux, “Securing Wireless Mesh Networks,” IEEE Wireless Communication, Vol.13, Issue 2, pp. 50-55, April 2006.

[5] T.K.L. Owens “Wireless Network Security 802.11, Bluetooth and Handheld Devices” NIST Special Publication 800-48, 2002. Available at http://www.governmentsecurity.org/articles/articles2/sp-800-48.pdf_fl/ (accessed July 2008).

[6] G.A. Marin “Network security basics,” IEEE Security and Privacy, Vol. 3, pp. 68-72, November/December 2005.

[7] Y. Zhang, J. Luo, H. Hu, “Wireless mesh networking, architectures, protocols and standards,” Auerbach Publications, Taylor & Francis Group, First Edition, NY, ISBN: 0849373999, 2006.

[8] D. Kalina ECE 478, March 2005: islab.oregonstate.edu/koc/ece478/05Report/ Kalina.doc.

[9] F. Xing, W. Wang, “Understanding Dynamic Denial of Service Attack in Mobile Ad hoc Networks,” IEEE Military communication conference (MILCOM), 2006.

[10] G. Glenn, “WLAN security challenges,” Security White Papers and Articles, March 2005. Available at http://www.securitydocs.com/pdf/3534.PDF (accessed July 2008).