

Threats and Vulnerabilities in Wireless Mesh Networks

Dr. M.S.Aswal¹, Paramjeet Rawat², Tarun Kumar³

¹. Vidya Engg. College, U.P., India

². IIMT Engg. College, U.P., India

³. Radha Govind Engg. College, U.P., India

E-Mail: {mahendra8367, paramjeet.rawat, taruncdac}@gmail.com

Abstract Wireless mesh networks (WMN) encompass a new area of technology set to play an important role in the next generation wireless mobile networks. WMN is characterized by dynamic self-organization, self-configuration and self-healing to enable flexible integration, quick deployment, easy maintenance, low costs, high scalability, and reliable services. Security of such a network has always been an issue. In this paper, we have analyzed the fundamental security requirements of WMN and the challenges faced by it. We have also discussed the vulnerable features and possible active threats in WMN along with few defense mechanisms against such threats. This paper serves a baseline for developing a secured, full-proof WMN which takes care of all types of attacks.

Index Terms— wireless network security, wireless mesh network, threats, wireless network counter measures.

I. INTRODUCTION

Wireless Mesh Network (WMN) [2] is an emerging new technology which is being adopted as the wireless networking solution for the near future. WMN has characteristics such as rapid deployment and self configuration. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Wireless Internet service providers are choosing WMNs to offer Internet connectivity, as it allows a fast, easy and inexpensive network deployment. Typical wireless mesh networks (WMNs) consist of mesh routers and mesh clients [3]. Mesh routers, which are static and power-enabled, forms a wireless backbone of the WMNs and interwork with the wired networks to provide multi-hop wireless Internet connectivity to the mesh clients. Mesh clients access the network through mesh routers. They can also directly mesh with each other. The development of this technology has to deal with the challenging security, architecture and protocol design issues. The state-of-the-art work is still insufficient for deploying sizable wireless mesh networks because important aspects such as network radio range, network capacity, scalability,

manageability, and security still remain open problems. In WMNs, as one component of the wireless technologies, security is one of the crucial components that needs due attention. The emergence of new applications of WMNs necessitates the need for strong privacy protection and security mechanisms of WMNs.

We give a brief overview of security requirements and challenges faced by WMN in section 2. In section 3, we look at the major security threats to WMN and in section 4 some defense mechanisms are discussed; finally, conclusion is made in section 5

II. SECURITY REQUIREMENTS AND CHALLENGES OF WMN

A. Security Requirements

To ensure the security of WMNs, the following major security objectives of any application have paramount importance.

- Confidentiality - It means that certain information is only accessible to those who are authorized to access it.
- Integrity - Integrity guarantees that a message being transferred is never corrupted. Integrity can be compromised mainly in the following two ways: Malicious altering – A message could be removed, replayed or revised by an adversary by a malicious attacker. Accidental altering - Such as a transmission error, goals on the network which is regarded as malicious altering.
- Availability - Availability ensures the survivability of network services despite of denial of service (DoS) attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable.
- Authenticity - Authenticity is essentially, assurance that participants in communication are genuine and not impersonators
- Non-repudiation - Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. It is useful for detection and isolation of a node with some abnormal behavior.

- Authorization - Authorization is a process in which an entity is issued a credential by the trusted certificate authority. It is generally used to assign different access rights to different level of users.
- Anonymity -Anonymity means that all the information that can be used to identify the owner or the current user, should be kept private and not distributed to other communicating parties.

B. Challenges

There are various challenges that we face in achieving security goals in WMN. First of all, wireless links in WMN makes it prone to active attacks, passive attacks and message distortion [1,4]. In WMNs, passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation [4]. Secondly, we have the probability of node being compromised due to the lack of physical protection. Hence, the system becomes unprotected to malicious attack from outside of the network as well as attacks launched from within the network. Thirdly, a WMN may be dynamic because of frequent changes in both its topology and its membership. This ad hoc nature can cause the trust relationship among nodes to change also. Finally, as WMN has memory and computational constraints, the traditional schemes for achieving security are not applicable. Study of WMN's specifics [11], led to the following critical security challenges.

III. THREATS AND VULNERABILITIES OF WMN

In this section, the main threats that violate the security criteria, which are generally known as security attacks, are analyzed.

1. Routing Protocol Threats

Wireless mesh networks may be susceptible to routing protocol threats and route disruption attacks. Many of these threats require packet injection with a specialized knowledge of the routing protocol; however, these threats are unique to wireless mesh networks and are summarized below:

- Black-hole. An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets, where attacking packets involve advertising routes as low-cost.
- Grey-hole. An attacker creates forged packets to attack and selectively drops, routes or inspects network traffic.
- Worm-hole. Routing control messages are replayed from one network location to another, which can severely disrupt routing.
- Route error injection. An attacker disrupts routing by injecting forged route error message to break mesh links. Relative to the other routing

attacks, this attack conceivably has high exploitability because it does not require detailed knowledge of the routing protocol state model. The risk associated with these threats depends on the routing technology or mesh network architecture.

- Identification of Compromised Nodes. For a WMN it is critical to identify the compromised nodes within it. First of all, the physical protection of the node is crucial. Then there is a possible attack by the removal or replacement of a node. This can be detected by the neighboring nodes when an unusual topology change is observed in the network. The second would be a passive attack on a node, which is very much difficult to identify. In the third case, the attacker might change the internal state of the node for attacking the routing algorithm etc. Finally, the fourth case can be cloning the captured device and installing replicas at some strategically chosen locations in the mesh network, which allows the adversary to inject false data or to disconnect parts of the WMN. This attack can seriously disrupt the routing mechanism.

In a mesh network, the exploitability of these threats may vary greatly – a network based on a known protocol such as AODV is more susceptible than a proprietary routing protocol. Similarly, a mesh network that uses message integrity checking for routing messages and device authentication will substantially decrease the threat risk (note that X.509v3-based trust or unique per hop security as per 802.11s offers greater security than basic security controls such as system-wide shared keys). These attacks have the potential to cause service degradation far beyond the reach of a single malicious transceiver.

2. Metro-Wifi Public Access Threats

Metro-WiFi threats depend on the deployed mesh products, as well as the network access strategy for the wireless operator. Mesh networks that provide free public access are susceptible to attacks based on the implication of open authentication (e.g., public access is synonymous with no pre-established trust to the wireless network). While many municipal wireless projects allow free Internet access, operators typically offer shared or graded service via a Layer 3 service gateway. Companies such as Pronto Networks offer solutions that simultaneously allow for protected access, a variety of service plans, and “walled-gardens” within the same network using SID/VLAN mapping with SSL-encrypted gateway registration and authentication.

3. Spoofing Of Wireless Infrastructure

Attacker used an “evil twin” or “man-in-the-middle” attack to execute an information disclosure threat. In an enterprise deployment, such attacks were

mitigated using EAP methods that allow mutual authentication between a client and the infrastructure

- Denial-of-service attack. A DoS attack could be launched at any layer of the network [9]. For instance, on the physical and media access control layers, an adversary could employ jamming signal to interfere with communication on physical channels. On the network layer, an adversary could interrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target of an adversary is the key management service, which is an essential service for any security framework.

- Something-of-Death Attack. While protocols serve a specific purpose, there is always the danger that bad implementations open yet another door for DoS attacks where a malicious attacker sends forged and mal-formed frames with the intention of crashing the AP under attack.

- Theft-of-Service Attack. An attacker could steal valid user credentials or performs paid-user session hijacking (e.g., “freeloading”). Many WiFi systems use a service gateway or captive portal to secure paid access – a captive portal uses SSL-secured Web page. After authentication, the captive portal authorizes the client to network access by registering the valid client MAC and IP addresses in the gateway. Alternatively, malicious users could relay traffic across the mesh network without traversing a network gateway (e.g., peer-to-peer traffic across the mesh backhaul). These attacks do not represent any new threats for mesh networks relative to existing WiFi hotspot services.

- Node Deprivation Attack. In node deprivation attack, the attackers target a single node and isolate it from taking part in the normal network operations. In WMN and IEEE 802.11, the nodes first authenticate itself with the mesh router or AP, and needs to de-authenticate [1] if the node has no more desire to use the network resources. The attacker could spoof the de-authentication message on behalf of the target node to stop it from using the network resources.

- Authorization Flooding on Backbone Devices. WMN and IEEE 802.11 nodes use Probe request frames to discover a wireless network, if a wireless network exist then the AP respond with Probe response frame. The clients select that AP which provides the strongest signal to it [4]. Here the attacker could spoof a flood of probe request frames presenting a lot of nodes searching for wireless network, which could seriously overload the AP or wireless mesh router. If the load exceeds, the threshold value will cause the AP or wireless mesh router to stop responding and may create service unavailability.

4. Physical Security Threats

- Conventional wireless network deployments were within an enterprise environment with physical and administrator control of the operator or agency. Outdoor wireless mesh networks require that the mesh access points be outside the physical control of the operator. Outdoor deployment poses more challenges for physical device security. Wireless mesh access points are mounted remotely on light-posts or externally on buildings, where a wide-area deployment may have several thousand such devices in an environment that is not within the physical and administrator control of the network operator. Wired mesh access points require network connectivity. Wired network access points sometimes require wired media backhaul, which may expose sensitive network connections.

- Battery Exhaustion. Battery exhaustion attack also known as ‘sleep deprivation attack’ is a real threat and is more hazardous than simple denial of service attacks. Attack on CPU computation may deny the availability of the service while battery exhaustion can disable the victim.

IV. RECOMMENDATIONS

Offering recommendations can often provide a false sense of security, as threats are difficult to anticipate and may often exploit previously unknown vulnerabilities. Securing wireless networks must always be treated carefully, mainly due to the inherent trust disparity in a wireless network.

A. Dos Attacks and Possible Countermeasures

DoS in any form against any network, is regarded as a severe attack. The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack. If launched against a single node either to exhaust its battery or to isolate it from the network operations. Selfish mesh router attack in WMN and rogue BS attack is used to make services unavailable for a target area in wireless broadband networks. Some possible countermeasure needs to be investigated to overcome it to some extent are:

- Cognitive radios implementation at physical layer needs to be investigated to handle the jamming and scrambling kind of attacks, which are common in all the broadband networks.

- Current encryption mechanisms used in these broadband networks are WEP, DES, and AES, which are vulnerable to eavesdropping kind of attack. Improved and efficient encryption mechanisms needs to be proposed exclusively for each of the broadband technology, as successful eavesdropping later on facilitate the attackers to launch DoS attacks.

- Intrusion detection mechanism can be used to detect and respond to most of the network layer threats particularly for WMN environment.

- A location detection mechanism based on the signal strength needs to be devised for the AP and wireless mesh router with the ability to identify a malicious node for flooding probe request and de-authentication kinds of attacks, same mechanism can be used for the IEEE 802.16 network to identify fake registration request flooding.
- Improved routing protocols are desirable particularly for the multi-hop WMN.

B. Cryptography & Digital Signatures

If the nodes can produce digital signatures and check them; then the solution is straight forward. While one node can verify the other nodes signature using public key cryptography, both nodes will establish a common secret key, using imprinting techniques, and will be able to accept messages protected by secret key. But many of the nodes in a WMN have computation and battery constraints (as discussed in section 2) due to which the verification process, which includes public key cryptography, may not be implemented. However, Elliptic Curve Cryptography (ECC) [10] provides some energy and computation efficient techniques in implementing cryptographic algorithm, which can be suitable for mobile clients.

C. Pair-Wise Key Sharing

In WMNs, symmetric cryptography is possible as it requires less computation than asymmetric cryptographic techniques. Or a better solution would be using the Diffie-Hellman (D-H) key exchange [12]. Diffie-Hellman(D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish shared keys over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

D. Secure Routing

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. There are two sources of threats to routing protocols. The first comes from external attackers. The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. To protect from such attacks we can exploit certain properties of WMNs to achieve secure routing. Like, Multipath routing [8] takes advantage of multiple routes in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. Even if certain routes are compromised, the receiver may still be able to validate messages.

V. CONCLUSION

In summary, the major security requirements, threats and vulnerability to WMN security are analyzed and finally few defense mechanisms are discussed. This paper can be used to give a baseline for building a tight security for WMNs.

REFERENCES

- [1] Muhammad S. Siddiqui and Choong Seon Hong, "Security Issues in Wireless Mesh Networks," IEEE International Conference on Multimedia and Ubiquitous Engineering, 2007
- [2] Ian F. Akyildiz, Xudong Wang and Weilin Wang, "wireless mesh networks: a survey," Computer Networks, vol. 47, pp. 445- 487, Jan. 2005.
- [3] W. Zhang, Z. Wang, S. K. Das, and M. Hassan, "Security Issues in Wireless Mesh Networks," In Book Wireless Mesh Networks: Architectures and protocols. New York: Springer, 2008
- [4] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks," In Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.
- [5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Communication, vol. 14, no.5, pp.85-91, Oct 2007
- [6] X. Gu and R. Hunt, "Wireless LAN Attacks and Vulnerabilities" In the Proceeding of IASTED Networks and Communication Systems, April 2005
- [7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking MobiCom 2002), pages 12–23, September 2002.
- [8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Efficient Security Mechanisms for Routing Protocols. In Proceedings of the 2003 Symposium on Network and Distributed Systems Security (NDSS '03), February 2003.
- [9] John Bellardo and Stefan Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In Proceedings of the USENIX Security Symposium, pages 15–27, August 2003.
- [10] M. Aydos, T. Tanyk, Ç. K. Koç, "High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor", IEE Pro.: Comms, Oct., 2001, pp 273-279.
- [11] R. L. Rivest, A. Shamir and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Comms of the ACM, v. 21-n.2, February 1978, pp. 120-126.
- [12] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, Nov, 1976, pp. 644-654.