Analysis of Secure Wireless Mesh Networks

Ritu Sharma[1] Dr. Prof. Deo Brat Ojha[2]

[1]Research Scholar CMJ University, Shillong, India

[2]Professor, R.K.G.I.T. , Ghaziabad, U.P.

Abstract - Wireless mesh networks (WMN) encompass a new area of technology set to play an important role in the next generation wireless mobile networks, and it is going to address the internet provision to user at low cost anytime from anywhere. 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, including solutions to the problems of intrusion detection. This paper serves a baseline for developing a secured, full-proof WMN

Key words: Intrusion detection, Network, Secure network routing, Security, WMNs, threats, attacks.

----------♦----------

INTRODUCTION

WMN encompass a new area of technology set to play an important role in the next generation wireless mobile networks, and it is going to address the internet provision to user at low cost anytime from anywhere. It has an ability to cover a wide geographic area with a limited transmit power accordingly. A WMN has several favorable features, such as dynamic self organizations, self-configuration, self-healing,

With the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad-hoc network)., easy maintenance, high scalability, and reliable services. A WMN is different from a mobile ad hoc network in that it relies on a high-speed back-haul network which is composed by WMN routers. A WMN optimizes network performance by using multiple radios. A WMN can provide gateways to the wired Internet and other wireless services. Due to its unique mesh structure, a WMN has an advantage over traditional MANET and wireless local area network in the areas of reliability, data throughput, ant jamming, and extensibility. WMN has been advocated as a cost-effective approach to support high-speed last mile connectivity and ubiquitous broadband access in the context of home network, enterprise networking, community networking, or metropolitan area network. The IEEE standard for mesh networking started as a Study Group of IEEE 802.11 in September 2003. Currently, the IEEE 802.11 is still in a development stage1, 2 In this paper, we first have a look into the security requirements n section 2) by WMN. In Section 3 we overview of challenges faced by WMN. In section 4 we look at the major vulnerabilities nd threats. In section 5 analysis of the unique attacks. In section 6 some defense mechanisms are discussed; finally, conclusion is made in section 7.

SECURITY REQUIREMENT OF WMNS

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 al 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 isissued 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.

CHALLENGES OF WMNS

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 . In WMNs, passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation condly, 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, led to the following critical security challenges.

THREATS AND VULNERABILITIES OF WMNS

There are two types of nodes in a WMN-the mesh router and the mesh client. MR provides a strong witch ability, minimum mobility, and ignorable battery restriction. Besides the traditional routing facility like gateway and bridge, the MR also supports routing functions specifically designed for a WMN as backbones of the WMN. Meanwhile, the MC could be designed with light architecture with the support of simplest routing ability and light-weighed communication protocols. Therefore,the MC only needs one wireless interface to achieve its function.Security is a vital problem in the design of a WMN. The client should have end-point-to-end-point security assurance.However, being different from a wired and traditional wireless network, a WMN could easily comprise various types of attacks. Even the WMN infrastructure like MR could be relatively more easily reached and modified by attackers.Therefore, appreciate security measures should be taken. Some common security threats in a WMN are listed below: The designer of the network should try to avoid these threats and keep the reliability of a WMN: **Physical Threat:** Generally, routers in wired networks are roperly protected. Therefore, the attack toward the routers in a wired network is difficult. However, the routers of a WMN are usually deployed outdoors like on roofs of buildings or on street mps. Therefore, physical protection to the routers of a WMN is very weak. This could cause the attacks to the routers like tempering the information in the router, stealing the private key for authentication stored in the router, or even replacing the router with a malicious one and hence the attacker will be able to connect to network as a legal node and send incorrect routing information. Therefore, secure routing protocols are essential to fight against this kind of attack. onventional wireless network deployments are 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, typically in environments that are not trustworthy (e.g., on a light-pole or an leased building exterior).

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.

Confidentiality and Integrity: Keeping the information sent out by the MR from being tempered or intercepted is very crucial in a WMN. This could be realized by employing encryptions in various layers. Hence finding a viable encryption policy for protecting confidentiality and integrity while minimizing the algorithm complexity and cost in management becomes the foremost problem. The existing WEP is not itable due to its inherent flaws.

Authentication in the WMNs: In order to prevent an unauthenticated node from connecting to the WMN, a strongauthentication mechanism is necessary. Every node joining theWMN should be able to verify the identities of others. In a WMN, the lack of terminal facilities causes the necessity of a distributed authentication mechanism to verify every MR or a centralized authentication mechanism by appointing one particular MR as the authentication server. In both the cases, the authentication should be based on security associations outside the IEEE 802.11.

Currently, using traditional asymmetric cryptography for authentication in a WMN is problematic due to the energy limitation and weak computational ability of the MC (usually devices like mobile phone). It is not practical for these devices to perform such complex computation required by asymmetric cryptography since it will cause a large time delay and accelerate the depletion of the batteries. Besides, this will create a new DoS method by asking MCs to run the authentication program repeatedly, which will take most of the CPU time and deplete the power of the MC.

Routing Protocol Threats: WMN 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 attracting packets involves 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 injected 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 (e.g., a replay attack is possible, and route errors are typically stateless). The risk associated with these threats depends on the routing technology or mesh network architecture. 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. Why are these attacks interesting? Unlike denial-of-service attacks on 802.11 MAC management frames or using RF interference, mesh disruption attacks have the potential to cause service degradation far beyond the reach of a single malicious transceiver.

Metro-Wi-Fi Public Access Threats: Metro-Wi-Fi___33 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 "walledgardens" within the same network using SSID/VLAN mapping with SSL-encrypted gateway registration and authentication

Spoofing of wireless infrastructure: An attacker uses an "evil twin" or "man-in-the-middle" attack to execute an information disclosure threat. In an enterprise deployment, such attacks are mitigated using extensible authentication protocol (EAP) methods that allow mutual authentication between a client and the infrastructure.

Denial-of-service attack: An attacker may either use IP flooding as well as attacking network services, or 802.11 MAC management attacks. The 802.11i-based link level security model supports authentication, key distribution and encryption for mesh management frames, where MAC management frame protection is not addressed within 802.11s.

Theft-of-service attack: An attacker steals valid user credentials or performs paid-user session hijacking (e.g., "freeloading"). Many Wi-Fi systems use a service gateway or captive portal to secure paid access – a captive portal uses SSL-secured Web page where users authorization credentials. 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 Wi-Fi hotspot services. However, mesh networking for municipal wireless has broadened the possible scope of usage and availability of public access networks.

POSSIBLE ATTACK TYPES IN THE WMNS

Denial of Service: The DoS attack is encountered either by accidental failure in the system or a malicious action. The conventional way to create a DoS attack is to flood any centralized resource so that it no longer operates correctly or stop working. A distributed DoS attack is even more sever threat to WMNs. DoS attack is launched by a group of compromised nodes who are part of the same

network and who collude together to bring the network down or seriously affect its operation.

Impersonation attack: This attack creates a serious security risk in WMNs. If proper authentication of parties is not supported, compromised nodes may be able to join the network, send false routing information, and masquerade as some other trusted nodes. A compromised node may get access to the network management system of the network; and it may start changing the configuration of the system as a legitimate user who has special privileges.

Routing attack: Routing attacks in WMNs:

Routing table overflow attack: an attacker attempts to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to resource exhaustion or DoS attack.

Byzantine attack: an invalid operation of the network initiated by malicious nodes where the presence of compromised nodes and the compromised routing are not detected. This attack will eventually result in severe consequences to the network as the network operation may seem to operate normal to the other nodes.

Location disclosure attack - this attack reveals something about the structure of the network to the locations of nodes such as which other nodes are adjacent to the target, or the physical location of a node.

Gray Holes and Black Holes: A black hole is a station that advertises its willingness to take part in a route but forwards no traffic. A gray hole is a more difficult to detect variety that conditionally decides on which traffic it will forward. One key property of gray and black holes is that they must attract traffic through themselves to be effective. Gray or black hole attacks might alter route replies or use a rushing attack to improve their routing metrics and become the preferred route for network traffic.

Wormholes Attacks (WHA): WHA can be severely problematic. With such attacks, the hostile adversary doesn't need to control any legitimate stations but still poses a significant outsider threat to the WMN's outing integrity. The WHA forms a tunnel connecting different parts of the network, thus tricking stations adjacent to one end of the wormhole into believing that they're neighbors with stations at the other end.

At first sight, a wormhole appears beneficial because it optimizes traffic flow across the mesh. The threat is that it also permits an adversary to conduct active traffic analysis and large scale DoS attacks.

Figure: 2 show an example WHA in which the hostile adversary has two stations linked to each other via a high-speed data link. The stations are located within radio range of the WMN, and traffic overheard by one end of the wormhole is relayed to the other where it's then rebroadcast and similarly in the reverse direction. In this example, station A would appear to have B, C, X, and Yas its direct neighbors, whereas Y would presume it has A, C,and X for its direct neighbors'. Station B would conclude that it has three two-hop routes to station X, but only the route B-> D >X Avoids the adversary. The threat posed by wormhole attacks is severe, and researchers have proposed several means of combating this threat. In essence such approaches seek to verify the authenticity of the transmission itself as well as the authenticity of the information actually exchanged. The connection between stations W1 and W2 creates a "wormhole" in the WMN topology analogous to the wormholes of theoretical physics.6

Rushing Attacks: In on-demand routing protocols, the attacker sends a lot of routing request packets across the networks in a short interval of time keeping other nodes busy from processing legal routing request packets

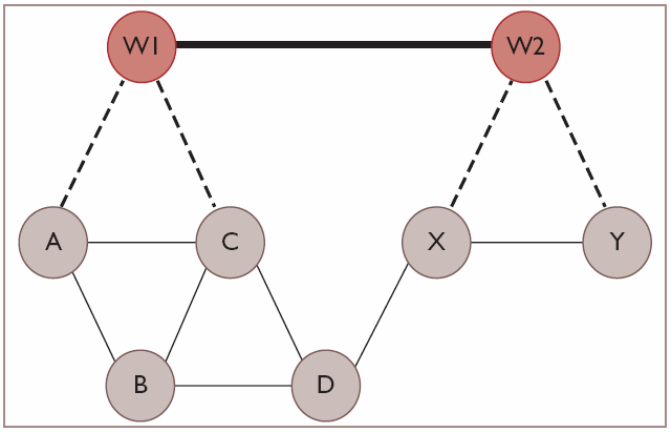

Figure-1 An example WHA

Table No. 1

Threats and Vulnerabilities in Different layer of WMN

(show in the table below)

LAYER ATTACKS

Application layer Repudiation, data corruption Transport layer Session hijacking, SYN flooding Networks layer Wormhole, black hole, Byzantine, flooding, resource consumption, location disclose attack Data link layer Traffic analysis, monitoring, disruption MAC(802.11) WEP

weakness Physical layer Jamming, interceptions, eavesdropping Multi-layer attacks

RECOMMENDATIONS

Dos, impersonation, replay; manin-the-middle 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.

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. 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 deauthentication 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.

Cryptography and 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) [8] provides some energy and computation efficient techniques in implementing cryptographic algorithm, which can be suitable for mobile clients.

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. 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 keycan then be used to encrypt subsequent communications using a symmetric key cipher.

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 10 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.

Intrusion Detection Systems: Because WMN has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in WMNs. Zhang11 gives a specific design of intrusion detection and response mechanisms. Marti proposes two mechanisms: watchdog and path rater, which improve throughput in the presence of nodes that agree to forward packets but fail to do so. In WMNs, cooperation is very important to support the basic functions of the network so the token-based mechanism, the credit-based mechanism, and the reputation-based mechanism can be used to enforce cooperation.

An ID collects activity information from all the nodes and then analyzes it to determine whether there are any activities that violate the security rules. Once the IDS determine that an unusual activity or an activity that is known to be an attack occurs, an alarm is generated to alert the security administrator.

In addition, IDS can also initiate a proper response to the malicious activity. The optimal IDS architecture for a WMN may depend on the network infrastructure itself On the basis of architectures IDS can be classified as:

Stand-alone Intrusion Detection Systems: IDS run on each node independently to determine intrusions.

Distributed and Cooperative Intrusion Detection Systems:

(Zhang et al.11) proposed an agent-based distributed and cooperative intrusion detection scheme) Every node participates in intrusion detection and response by having an IDS agent running on them. An IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

The IDS agent can be structured into six pieces including local data collection, local detection engine, cooperative detection engine, local detection engine, local response, global response, and secure communication. Figure: 2 shows a conceptual model for an IDS agent.

Hierarchical Intrusion Detection Systems: Cluster heads act as control points to provide the functionality for its child nodes. To have separate IDS on each mobile client is not feasible that is why, Distributed IDS and Hierarchical IDS are suitable for WMNs.

CONCLUSION

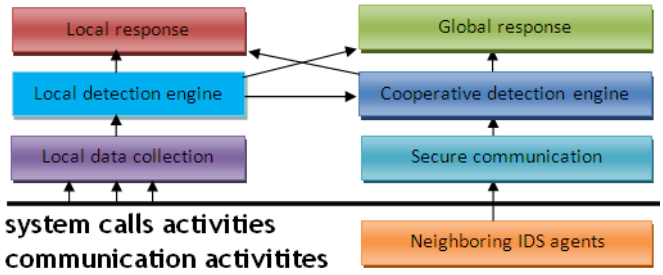

Figure-2 2 IDS Agents

In this paper, the major security requirements, threats and vulnerability to wireless mesh networks

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 wireless mesh networks.

REFERENCES

1. Akyildiz I.F., Wang X. and Wang W., Wireless mesh networks: a survey, *Comp Net*, **47(4)**, 445-87 **(2005)**

2. Camp J. and Knightly E., The IEEE 802.11s extendedservice set mesh networking standard, *IEEE CommunicatMagaz*, **46(8)**, 120-6 **(2008)**

3. Muhammad S. Siddiqui and Choong Seon Hong,Security Issues in Wireless Mesh Networks, IEEE International Conference on Multimedia and Ubiquitous

4. Zhang W., Wang Z., Das S.K. and Hassan M., Security Issues in Wireless Mesh Networks, In Book Wireless Mesh Networks: Architectures and protocols, New York, *Springer* **(2008)**

5. Rivest R.L., Shamir A. and Adleman L.M., A Method for Obtaining Digital Signatures and Public- Key Cryptosystems, Comms of the ACM, **21(2)**, 120-126**(1978)**

6. Steve Glass, Marius Portmann and Vallipuram, securing wireless mesh networks, IEEE computer society-10987801-2008@IEEE

7. Hu Y.C., Perrig A. and Johnson D.B., Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, Proc. 2003 ACM Workshop on Wireless Security, ACM Press, 30–40 **(2003)**

8. Aydos M., Tanýk T., Koç C.K., High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor, IEEPro.: Comms, 273-279 **(2001)**

9. Diffie W., Hellman M., New Directions in Cryptography, IEEE Trans., on IT, 644-654 **(1976)**

10. 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) **(2003)**

11. Zhang Y., Lee W. and Huang Y., Intrusion Detection Techniques for Mobile Wireless Networks in ACM/Kluwer Wireless Networks Journal (ACMWINET), **9(5)**, **(2003)**

12. Marti S., Giuli T., Lai K. and Baker M., Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, in proceeding of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 255-265 **(2000)**

13. Albers P., Camp O., Percher J., Jouga B., L.M., and Puttini R., Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. 80