Attacks and their Counter Measures in Wireless Mesh Networks

Anil Kumar Gankotiya[1], Sahil Seth[2], Gurdit Singh[3]
Department of Computer Science,
PEC University of Technology,
Chandigarh, India
[1]anilgankotiya@ieee.org, [2]sahilseth@ieee.org, [3]gurditsingh@ieee.org

Abstract— **Wireless mesh networks (WMNs) have emerged as a key technology for next-generation wireless networking. Because of their advantages over other wireless networks, WMNs are undergoing rapid progress and inspiring numerous applications. However, many technical issues still exist in this field. In order to provide a better understanding of the research challenges of WMNs, this article presents a detailed investigation of current state-of-the security issues in WMNs. Open research issues in protocol layer is also discussed, with an objective to spark new research interests in this field.**

***Keywords*— Medium Access Control, Routing, Wireless Mesh Networks, WMN Security**

I. INTRODUCTION

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs) [7], has emerged recently. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

Conventional nodes (e.g., desktops, laptops, PDAs, Pocket PCs, phones, etc.) equipped with wireless network interface cards (NICs) can connect directly to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help the users to be always-on-line anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi) [4], and worldwide inter-operability for microwave access (WiMAX) [5], WiMedia [6] networks. Consequently, through an integrated WMN, the users of existing network can be provided with otherwise impossible services of these networks.

This work was done at Cyber Security Research Center, situated at PEC University of Technology, Chandigarh and supported by Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi, under the grant for the Project *"Investigate, Explore & Implement security aspects in existing protocols in Wireless Mesh Network.*

Sahil Seth is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091+98786-72540, email: sahilseth@ieee.org.

Anil Gankotiya is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091+99882-11382, email: anilgankotiya@ieee.org.

Gurdit Singh is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091-98554-30628 email: gurditsingh@ieee.org.

WMN is a promising wireless technology for numerous applications [3], e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It is gaining significant attention as a possible way for cash strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments. With the capability of self-organization and self configuration, WMNs can be deployed incrementally, one node at a time, as needed. Deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc network routing protocols, IEEE 802.11 MAC protocol [12], wired equivalent privacy (WEP) security [3], etc. Several companies have already realized the potential of this technology and offer wireless mesh networking products. However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; the throughput drops significantly as the number of nodes or hops in a WMN increases. Similar problems exist in other networking protocols. Consequently, all existing protocols from the application layer to transport, network MAC, and physical layers need to be enhanced or re-invented.

OUTLINES

The remainder of the paper is organized as follows. In Section 2, we present the architectures of WMNs. Critical design factors are summarized in Section 3. In Section 4, difficulties in providing the security in WMN are discussed. Possible Attacks in WMN are emphasized in Section 5. We discuss typical attacks on MAC Layer and on Network Layer in Section 6-7. Characteristics of WMN Security mechanism are presented in Section 8. In section 9-10 will discuss the security and security model in WMN. In section 11-12 authentication of mesh router and possible solutions to authentication are discussed. Secure Routing and possible solution for sure routing been highlighted in Section 13-14. The paper is concluded in Section 15.

II. NETWORK ARCHITECTURE

WMNs [8] consist of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared with a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multi-hop communications. Optionally, the medium access control (MAC) protocol in a

mesh router is enhanced with better scalability in a multi-hop mesh environment.

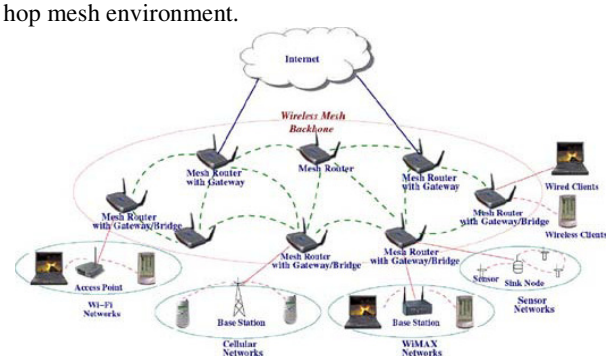

Figure 1: Infrastructure/backbone WMNs

A. *Hybrid WMNs*

This architecture is the combination of infrastructure and client meshing as shown in Fig 2. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid mesh network [13] architecture will be the most applicable case in our opinion.

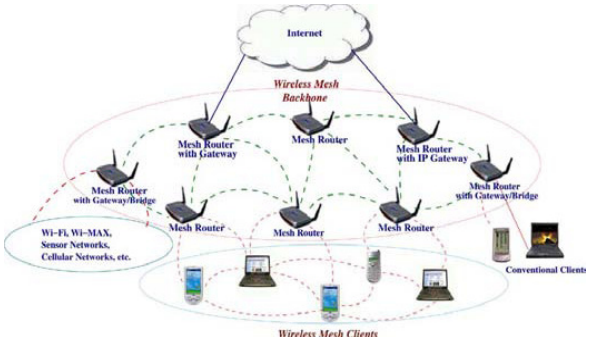

Figure 2: Hybrid WMNs

III. CRITICAL DESIGN FACTORS

The critical factors influencing the performance of WMNs are summarized as follows:

A. *Radio Techniques*

Many approaches have been proposed to increase capacity and flexibility of wireless systems in recent years. Typical examples include directional and smart antennas, multiple input multiple output (MIMO) systems, and multi-radio/multi-channel systems.

B. *Scalability*

Scalability is a critical requirement of WMNs. Without support of this feature, the network performance degrades significantly as the network size increases. For example, routing protocols may not be able to find a reliable routing path, transport protocols may lose connections, and MAC protocols may experience significant throughput reduction. To ensure the scalability in WMNs, all protocols from the MAC layer to the application layer need to be scalable.

C. *Mesh Connectivity*

Many advantages of WMNs originate from mesh connectivity. To ensure reliable mesh connectivity, network self-organization and topology control algorithms are needed. Topology-aware MAC and routing protocols can significantly improve the performance of WMNs.

D. *Broadband and QoS*

Different from classical ad hoc networks, most applications of WMNs are broadband services with heterogeneous QoS requirements. Thus, in addition to end-to-end transmission delay and fairness, more performance metrics, such as delay jitter, aggregate and per-node through-put, and packet loss ratios, must be considered by communication protocols.

E. *Ease of Use*

Protocols must be designed to enable the network to be as autonomous as possible. In addition, network management tools need to be developed to efficiently maintain the operation, monitor the performance, and configure the parameters of WMNs. These tools, together with the autonomous mechanisms in networking protocols, enable rapid deployment of WMNs.

F. *Compatibility and Inter-operability*

In WMNs it is a default requirement to support network access for both conventional and mesh clients. Therefore, WMNs need to be backward compatible with conventional client nodes. This demands that mesh routers need to be capable of integrating heterogeneous wireless networks.

G. *Security*

Although many security schemes have been proposed for wireless LANs in recent years, they are still not fully applicable for WMNs. For instance, there is no centralized trusted authority [9] to distribute a public key in a WMN due to the distributed system architecture. The existing security schemes proposed for ad hoc networks can be adopted for WMNs. However, most of the security solutions for ad hoc networks are still not mature enough to be implemented practically. Moreover, the different network architectures between WMNs and ad hoc networks usually render a solution for ad hoc networks ineffective in WMNs.

IV. DIFFICULTIES IN PROVIDING SECURITY IN WMNS

There are some difficulties in providing the security in WMN which are describes as follows:

A. *Shared Broadcast Radio Channel*

It is the security problem in the WMN; as the radio channel is same for the sending and receiving the data so there is the possible attack like MAC Layer eaves-dropping or the reply back.

B. *Lack of association*

It is another security problem in WMN as the authentication is poor in the WMN. All of the authentication is done via sending the shared keys, may be by using WEP [14] or WPA2 [14] technology. In the next topics we will see how these security issues are removed in WMN.

C. *Physical Vulnerability*

In this is the main problem lies in the WMN. The problem is like the replacement of the mesh router.

D. Limited Resource Availability

In this, as the resource is limited in the WMN so there is limitation of mesh router and client and the communication overhead.

V. POSSIBLE ATTACKS IN WMNS

Some of the possible attacks in WMN are listed below:

A. External attacks

They are those which are launched by intruders who are not part of a WMN and try to gain illegitimate access to the network. Thus by this they can raise the computation power of the network and can degrade the performance of the network. Some attacks that are possible in the WMN by the intruder in the network as: DoS (Denial of Service) attack [2]. This attack is the major problem in WMN as it sends the false messages in the network, thus making the network to choke down and making the resources unavailable. Thus detecting the DoS attacks in the networks is still in research.

Other external attack in the WMN is the encryption and authentication. According to this the authentication in the network is done by the access points, the authentication are done by the access points is may be using the WEP or using WPA technology; as these algorithms are found out to be compromised by using some hacking software. So these algorithms need to be revised.

Encryption is done while sending the data been encrypted by using the shared key. As in the network all of the packets been encrypted with their shared key, so there is the possibility of the attack by guessing the shared key, so that the message can be forged.

B. Internal Attack

Internal attack is launched by the internal nodes which are a part of the WMN, they may be the selfish nodes or the malicious nodes that have been possibly been compromised by the attackers. By this they have access to all of the keying and authentication information.

So to detect the attack internally some mechanisms should be employed to detect and isolate the misbehaving nodes. The example of the mechanism is the use of the IDS (Intrusion Detection System).

VI. TYPICAL ATTACKS ON MAC LAYER

The typical attacks on the MAC layer can be:

A. *Eavesdropping*

Network Eavesdropping or network sniffing is a MAC layer attack consisting of capturing packets from the network transmitted by others computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.

The attack could be done using tools called network sniffers. These tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling.

Network Eavesdropping is a passive attack which is very difficult to discover. It could be identified by the effect of the preliminary condition or, in some cases, by inducing the evil system to respond a fake request directed to the evil system IP but with the MAC address of a different system.

B. Link Layer Jamming Attack

It is the attack generated with the regular transmits MAC frames headers with no payload on the transmission channel, which conform to the MAC protocol. This may leads to the DoS or energy depletion for the legitimate users.

C. MAC Spoofing Attack

Eavesdrop on the network to determine the MAC addresses of legitimate devices and masquerade as a legitimate user. This leads to illegal access or DoS.

D. Reply attack

Copy or eavesdrop data between two nodes and then transmit these legitimate messages at a later stage to masquerade as a legitimate user.

VII. TYPICAL ATTACKS ON NETWORK LAYER

Some typical attacks which can be done on the network layer are:

A. Control plane attack

This is the major attack in the WMN as the attacker makes the routes unavailable or control the routing path. The attacker just targets the routing functionality of the network layer. The examples of the attack are:

1) *Rushing Attack:* It is launched by a malicious node who forwards the Route Request message before any other intermediate node by ignoring the specified delay.

2) *Wormhole Attack:* Two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium.

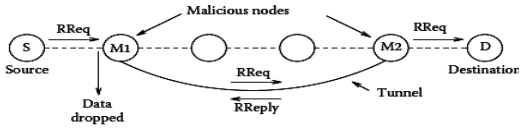

Fig. 3 Wormhole Attack

3) *Black Hole Attack:* The malicious node always replies positively to a Route Request although it may not have a valid route to the destination.

Almost all the traffic within the neighborhood will be directed toward the malicious node, which may drop all the packets,

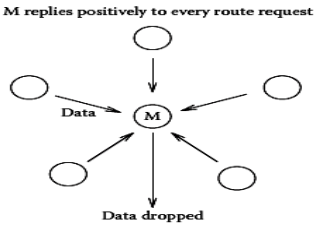

Fig. 4 Black Hole Attack

B. Data plane attacks

This attack is launched by the selfish node or the malicious node which is been compromised by the attacker by dropping packets or injecting the malicious data into the network. This may lead to the DoS attack in the network. So the main objective of the attacker is to cause the DoS to legitimate user by making the user data undeliverable.

In the later section we will discuss that how we can secure the WMN from the various attacks that we discussed above.

VIII. CHARACTERISTICS OF WMN SECURITY MECHANISMS

There are some characteristics of WMN security mechanisms which are as follows:

A. *Robust Trust Establishment Mechanism*

The trust establishment mechanism should be robust against internal selfish and malicious behavior.

B. *Differentiate Mesh Router & Mesh Client*

For the Mesh Routers and the Mesh Clients different Security requirements and the constraints are required.

C. *End-to-end Security Services*

To counteract the selfish and malicious behavior of the en-route nodes, the WMN must provide the end-to-end security services, in addition to a per-link basis.

D. *Accountability*

Ensure the WMN nodes behave according to the protocol specification even if the nodes make independent decisions about routing and channel assignment.

IX. SECURING WMNS

We can secure our network by using the appropriate measures like using the IDS in our system.

A. *Intrusion Prevention*

We can secure our network by running the security services that stop the attacker from intruding into the network and launching the attack on the network these including authentication, access control, data confidentiality, data integrity, and non-repudiation.

B. *Intrusion Detection*

In this we have to identify the illegitimate activities, which may be the consequence of an attack or may lead to an attack. Most of the security mechanisms and protocols follow the prevention approach.

X. SECURITY MODEL IN WMNS

Below approach is the security provision in the intrusion prevention.

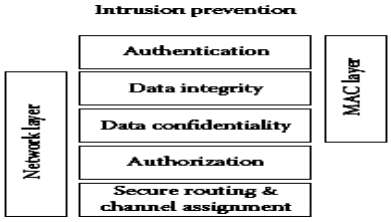

Fig. 5 Intrusion Prevention

Below approach is the intrusion detection and automated response.

Fig. 6 Intrusion Detection and Automated Response

XI. AUTHENTICATION OF MESH ROUTER

Authentication of the router depends upon the following points:

A. *Basic Idea*

- Each mesh router has a certified public/private key pair assigned by the administrative entity
- Each router pre-deployed with all the other routers public keys without resorting to a Certificate Authority.
- Revocation or adding new node by broadcast.

B. *Trade of Between Storage-usage and Complexity*

- To improve the storage-usage situation by letting each node carry a one-way hash value of the public keys.
- To further improve the storage-usage by Markel Tree.

XII. POSSIBLE SOLUTIONS TO AUTHENTICATION

Some possible solution to the authentication is shown below:

A. *Public key cryptography for authentication of mesh routers*

- Less resource constraint, robust to internal attacks.
- Using one-way hash function to conduct public key authentication instead of a Certificate Authority (CA).

B. *Dual Authentication Model adopted for authentication of authorized mesh clients*

1) Authentication of the mesh clients should be performed during mesh clients' roaming across different wireless mesh routers.

2) Applying 802.11X in WMNs

XIII. SECURE ROUTING

All of the routing is done on the third layer that is the network layer. So we have to prevent the network layer from the control plane attack.

There are some approaches for the secure routing:

A. *Multi-path Routing*

- Provide alternate paths between the source and destination when attacks happen.
- Increase the throughput.
- Work with intrusion detection mechanisms.

B. *Secure the routing protocols*

Compelling each node to follow the routing protocol; the common idea is to establish the trust between the participating nodes and the control message integrity and confidentiality. So there are some of the existing secure routing protocols which can be used to secure our routing in WMN:

1) *SRP [11]:* The Route Request and Route Reply messages are protected by message authentication code (MAC) for authentication of the originating node. The IP address of the intermediate nodes is also added in the Route Request message for cross validation.

2) *SAODV [1]:* It uses digital signatures to authenticate all the immutable fields of Route Request and

Route Reply messages. The hop count field is secured using hash-chains on per-link basis.

XIV. POSSIBLE SOLUTION FOR SECURE ROUTING

There are some possible solutions for securing the routing which are as:

A. *Pro-active routing protocols*

- Table-driven.
- Transmission Overhead: Nodes periodically broadcast routing information to keep the routing tables up-to-date.

B. *Re-active routing protocols (On-demand)*

- A sender node requests to establish a route only when data are needed to be sent.
- Delay in route finding

C. *Sender Authentication*

Each mesh router should sign the non-mutable part of a routing packet when they generate it. By this way, any impersonating routing information generated either by the external or internal attackers will be discarding.

D. *Routing Information Authentication*

Each mesh router should conduct an end-to-end authentication for the hop value (which may be different routing metrics in different routing protocols) in the routing packet before update its route table.

XV. CONCLUSION

The capability of self-organization in WMNs reduces the complexity of network deployment and maintenance, and thus, requires minimal upfront investment. The backbone of WMNs provides a viable solution for users to access the Internet anywhere anytime. It can also enhance the reliability of the mobile ad hoc network of mesh clients. WMNs enable the integration of multiple wireless networks.

WMNs can be built up based on existing technologies. In this paper we investigated various security challenges facing by WMNs and address the typical MAC layer and network layer attacks. We enlist some characteristics that differentiate the WMN security mechanisms from the existing security mechanisms for wired and ad hoc networks. By considering the existing security mechanisms and the characteristic requirements of WMNs, we suggest our security solutions for two important security services in WMNs, authentication and secure routing.

ACKNOWLEDGEMENT

The authors would like to thank Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi, for funding the Project *"Investigate, Explore & Implement security aspects in existing protocols in Wireless Mesh Network",* under which this work has been done.

REFERENCES

[1] D. Cerri and A. Ghioni, "*Securing aodv: the a-saodv secure routing prototype*," *Communications Magazine, IEEE*, vol. 46, no. 2, pp. 120-125, February 2008.

[2] Blum, J.J. Neiswender, A. Eskandarian, A. Pennsylvania State Univ., Middletown, PA; "*Denial of Service Attacks on Inter-Vehicle Communication Networks*" Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference, Oct. 2008, pp : 797-802.

[3] Martin Beck, Erik Tews,"*Practical Attacks against WEP and WPA*", Nov 2008.

[4] Bruno, R. Conti, M. Gregori, E. "*Mesh networks: commodity multihop ad hoc networks*", IEEE Communications Magazine, March 2005, Volume: 43, Issue: 3, pp: 123- 131.

[5] The Wi-Fi Alliance. Available from: <http://www.wi-fi.org/>.

[6] The WiMAX Forum. Available from: <http://www.wimaxforum.org/home>.

[7] The WiMedia Alliance. Available from: <http://www.wimedia.org/>.

[8] I. F. Akyildiz, X. Wang and W. Wang, '*Wireless Mesh Network: A Survey*' in Computer Networks and ISDN Systems, Volume 47, Issue 4, March 2005.

[9] Mesh Networking Forum, "*Building the business case for implementation of wireless mesh networks*", Mesh Networking Forum 2004, San Francisco, CA, October 2004.

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "*Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks*," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[11] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, "*A secure routing protocol for Ad-hoc networks*," Proc. Of IEEE ICNP, 2002.

[12] Pablo Brenner, "*A Technical Tutorial on the IEEE 802.11 Protocol"*, July 1997.

[13] Raheleh B. Dilmaghani , Ramesh R. Rao *,"Hybrid Wireless Mesh Network Deployment", WiNTECH'06,* September, 2006, Los Angeles, California, USA.

[14] Halil Ibrahim Bulbul, Ihsan Batmaz, Mesut Ozel, *"Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols"*, Adelaide, Australia, 2008.

Anil Gankotiya is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091+99882-11382, email: anilgankotiya@ieee.org.

He is working as student member of Cyber Security Research Center situated at PEC University of Technology and working on the project *"Investigate, Explore & Implement security aspects in existing protocols in Wireless Mesh Network."* funded by Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi.

Sahil Seth is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091+98786-72540, email: sahilseth@ieee.org.

He is working as student member of Cyber Security Research Center situated at PEC University of Technology and working on the project *"Investigate, Explore & Implement security aspects in existing protocols in Wireless Mesh Network."* funded by Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi.

Gurdit Singh is currently doing thesis work at Cyber Security Research Center in Department of Computer Science, PEC University of Technology. (Mob: 0091-98554-30628 email: gurditsingh@ieee.org.

He is working as student member of Cyber Security Research Center situated at PEC University of Technology and working on the project *"Investigate, Explore & Implement security aspects in existing protocols in Wireless Mesh Network."* funded by Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi.