ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

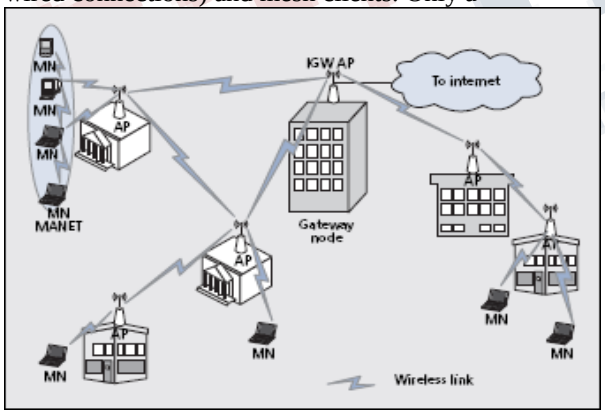
Critical Security Issuesand Challengesof Wireless Mesh Networks

[1] MrsM.S.Joshi [2] MrsA.A.Bakare [3] MrsV.V.Pangave [4] MrsV.C.Kulkarni [5] Mrs.S.S.Navale
[1][2][3][4][5] MAEER'S MIT Polytechnic

Abstract: **In this paper, we investigate the principal issues and challenges pertaining to the security of Wireless Mesh Networks (WMNs). We study the threats a WMN faces and the security goals to be achieved. WMN is a new wireless networking model. 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. The main challenge in design of these networks is their vulnerability to security attacks. WMNs offer an easy and economical alternative for providing broadband wireless internet connectivity and could be termed as Web-in the sky. These networks have the ability to organize and configure themselves dynamically. These networks provide improved flexibility, efficiency and coverage as compared to the conventional networks. In place of a wired connection, WMN forms a wireless connectivity thus eliminating the need for extensive cabling. They are based on multihop communication patterns that form a dynamically connected network. However,multihop wireless communication networks are facing limitations such as a low throughput and they are also plagued with several security issues.**

I. INTRODUCTION

WMNs have the potential to provide high speed internet connectivity over a sizeable geographical area at a much lower cost than the conventional wireless network. They consist of mesh routers (access points that do not have wired connections) and mesh clients. Only a



subset of access points (APs) is connected to the wired network. All the APs that are connected to the wired network are called Internet gateways or mesh point (MP). The mesh routers connect to the mesh points using multihop communication. These networks are extremely reliable as each node is connected to several other nodes, such that,if a node drops out of the network due to hardware failure or any other reason then its neighbors simply find an alternative path to reach the destination. The data hops from one device to another device until it finally reaches the destination.

II. CHARACTERISTICS OF WMNs

Mesh routers are static:Route selection should be focused on discovering high-bandwidth links with minimum interference.

Mesh routers have no power constraints: Mesh routers have abundant power at their disposal. Hence the routing protocol should target at increasing the channel bandwidth.

Mesh routers are equipped with multiple radios: Mesh routers are equipped with multiple radios,thus allowing simultaneous transmission and reception using intelligent channel assignment.

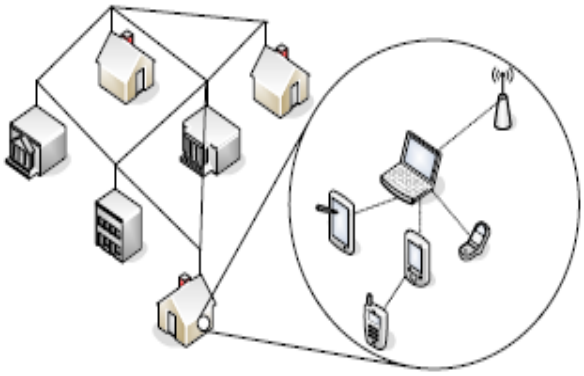
Traffic volume and number of users:WMNs provide high bandwidth broadband connections to a large number of users.

Traffic model:Traffic in WMNs is mostly between the MRs and THE IGWs (Internet gateways).

WMNs are extremely reliable, as each node is connected to several other nodes. Extra capacity can be installed by simply adding more nodes. Elements such as network architecture, network traffic, network topology, number of channels, transmission power decide the capacity of a WMN.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016



III. CRITICAL ISSUES IN WMNs

Physical layer issues:

As the distance increases, the SNR decreases, as the signals encoded using higher modulation techniques cannot be decoded at the receiver. Due to the distributed nature of wireless networks, different nodes maytransmit signals simultaneously, generating interference to other receivers. Interference increases with the increasing number of nodes. Most existing topology controlschemes have used omni directional antennas. Therefore, when the power is reduced, the transmission range is also decreased in all directions, which leads to shorter hop distance and lower interference. Topology control is also essential as the nodes can be placed anywhere.

Media Access Issues:

Some nodes may remain starved due to hidden and exposed terminals in a multihop environment. An ideal MAC protocol should provide fair access to all nodes accessing the channel. Due to the distributed nature of wireless networks, different nodes maytransmit signals simultaneously, generating interference to other receivers. In general, interference may lead to collisions and consequently data retransmissions at the medium access control (MAC) layer.

Secondly, there is a 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 adhoc 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. Quality of Service (QoS) provisioning is essential as the WMNs may support applications like broadband Internet access, and real time applications like video conferencing.

Quality of Service, in general, QoS refers to the guarantee of bandwidth (or throughput/data rate) and end-to-end delay.

Routing Issues in WMNs:

The focus of routing protocols in WMNs lies in identifying a best possible route between the gateways and the mesh clients.The link quality may be affected by the distance between the transmitter and the receiver. As the distance between the transmitter and receiver increases,SNR decreases thus affecting the decoding process at the receiver.

IV. SECURITY ISSUES

Security in WMNs explores key security challenges set in diverse scenarios, as well as emerging standards that include authentication, access control and authorization, attacks, privacy and trust, encryption, key management, identity management, DoS attacks, intrusion detection and prevention, secure routing, and security policies. There are two kinds of security attacks on a WMN. They are active attacks and passiveattacks.

Layer	Threats
Application	Logic errors, buffer overflows, privilege escalation
Transport	DNS spoofing, session hijacking, traffic injection
Network	Black/gray/worm holes, misrouting, rushing attacks
Data-link	Traffic flooding, virtual jamming, man-in-the-middle
Physical	Collision jamming, device tampering

An active attack is conductedto intentionally disrupt the network.A passive attack, like a selfish node attack or eavesdropping, drops packets with a selfish motivation to prioritize its packets and does not cause any

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

intentional damage to the network. The openness of WMN network makes it vulnerable to intruders, both external and internal. An external intruder may disrupt the routing by partitioning the network. An inside attacker in the form of compromise notes may go undetected. An intruder can render the network dysfunctional in various ways such as misrouting of data, failing to forward traffic, executing of denial of service attack, manipulating the content of payload. Hence the fundamental security primitives of authentication, integrity and confidentiality are very essential for the correct functioning of WMNs. Authentication refers to the verification of identities of the communicating entities. Authentication allows one station to prove its identity to the other station.Integrity refers to the validity of the original message to guarantee that it has not been tampered with by an intermediate node, and confidentiality refers to the establishment of a secure channel to transmit Cipher text. There are two dimensions to security in WMNs which consists of MPs and Mesh clients. As the interconnected MPs form the backbone of the network, highest level of security is required here and all MPs should be authenticated in the network. An equal amount of attention has to be paid to mesh clients to prevent intrudersin the network. This can be implemented using authentication servers like RADIUS and 802.1 x. 802.11 MAC protocolcurrently being used in WMNs which are susceptible to several security flaws.

V. CRITICAL SECURITY OTHER CHALLENGES

1. Detecting the Corrupted Nodes: It is very essential to detect the corrupted nodes in a WMN. 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 sensed 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 that of cloning the captured device by installing replicas at some specifically chosen locations in the mesh network, which allows the enemy to inject false data or to disconnect parts of the WMN. This attack can seriously disrupt the routing mechanism.

2. Multi-Hop Routing: The attacker can disrupt the routing mechanism and malfunction the WMN by inserting false routing messages. To alter the routing mechanism, the attacker may tamper with the routing messages, modify the state of one of the nodes, use replicated nodes

3. Fairness: In WMNs the nodes act as message repeaters or forwarders, therefore output signal obtained by a node significantly depends upon the topology of the network and nodes surrounding that node. The fairness issue in WMNs is closely related to the number of hops between the nodes, which indicates that if the adversary manages to increase the number of hops between sender and receiver nodes, it can decrease the bandwidth.

4. Availability: Availability ensures the survivability of network services despite attacks. Long-term Denial of Service (DoS) attacks can severely hamper a network's ability to continue.The availability in a WMN can be compromised by following ways.Availabilityensures that the system remainsoperational even in the presence of malicious or faulty nodes. The common threat to availability is a denial of service (DOS) attack.

5. Signal Jamming: An attacker can attack on the physical and MAC layers, of the network by employing jamming to interface with communication on physical channels.

6. Denial of Service (DoS): A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internetsite or service from functioning efficiently or at all, temporarily or indefinitely. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legal traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.An attacker can launch a DoS attack at any layer of the WMN. There are many ways of forcing a DoS attack. A common technique is to flood the target system with requests. The target system becomes so

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

overwhelmed by the request that it could not process normal traffic. This attack is called distributed DoS and it is very difficult to counter.

7. Black hole attack: In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

8. Wormhole attack: A wormhole attack is one of the mostsophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network.The seriousness of this attack is that it canbe launched against all communications thatprovide authenticity and confidentiality.

9.IP Spoofing: IP spoofingis the creation of TCP/IP packets with somebody else's IP address in the header. Routers use the destination IP address to forward packets, but ignore the source IP address. The source IP address is used only by the destination machine, when it responds back to the source. When an attacker spoofs someone's IP address, the victim's reply goes back to that address. Since the attacker does not receive packets back, this iscalled a one-way attack or blindspoofing. To see the return packets, the attacker must interceptthem.

The types of spoofing are, (a) IP spoofing where attacker uses IP address of another computer to acquire information or gain access (b) email spoofing where attacker sends email but makes it appear to come from someone else and (c) web spoofing where attacker tricks web browser into communicating with a different web server than the user intended.

10. Battery Exhaustion: Battery life is the most critical parameter for many nodes in a wireless mesh network. Battery exhaustion attack also known as 'sleep deprivation attack' is a real threat and is more hazardous than simple denial of service attacks.

11.Authenticity: Authenticationprovides the communicating parties with a way to verify their identity. Authenticity enables a node to ensure the identity of the peer node it is communicating with. Without authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes. With the implementation of the concepts such as ubiquitous system, the abundance of networking nodes is reasonable. All these nodes should have an authentic communication within the network. Authentication mechanism works on the basis of public key cryptography, using a node which has better computational power. The main controller of the user can provide authenticity on the behalf of the node and within the local network authenticity is ensured by secure transient association.

12. Imprinting: The mechanism by which devices acquire the self-signed mediator's certificate is called imprinting. A network node will recognize as its owner the first entity that sends it a secret key. As the new node receives this key, the device willalways stay faithful to its owner. If the new node is surrounded by more than one node then the first one which sends the key would become the owner.

13. Integrity: Integrityenables the recipient of a message to verify that a message was not altered while in the network. The concept of integrity ensures that the contents of data or correspondences are preserved intact through the transfer from sender to receiver. Integrity embodies the guarantee that a message sent is the messagereceived, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways (a) by the intentional alteration of the data for vandalism or revenge or by the unintentional alteration of the data caused by operator input, computer system, or (b) faulty application errors.

14.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 due to which the verification process, which includes public key cryptography, may not be implemental.

15.Confidentiality: Confidentialityguarantees that communicated data is accessible only to the intended recipient(s).The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. For confidentiality, authenticity needs to be implemented first. It is pointless to attempt to protect the secrecy of a communication without first ensuring that one is talking

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

to the right principal. Once, authenticity is achieved, confidentiality is simply a matter of encrypting the session.

VI. SECURITY GOALS

WMNs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To secure a WMN, we consider the following attributes.

Secure Routing:

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Several routing protocols for WMNs have been proposed. A majority of these protocols assume a trustworthy collaboration among participating devices that are expected to abide by a "code-of-conduct". But there lie several security threats, some arising from shortcomings in the protocols, and others from the lack of conventional identification and authentication mechanisms. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing.

The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. To defend against the first kind of threats, nodes can protect routing information in the same way theyprotect data traffic. However, this defense is ineffective against attacks from compromised servers. Detection of compromised nodes through routing information is also difficult in a WMN because of its dynamic topology changes.

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 afixed wired network are not applicable in WMNs mechanisms. IDS 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 isknown to be an attack occurs, an alarm is generated to alert the security administrator. In addition, IDS can also initiate a proper response to themalicious activity.

Trust Management :

Trust and Security are two mutually dependant concepts, which cannot be segregated. For example trust cannot be assured without the scrutiny of secure communication, similarly security attributes such as cryptography requires trusted key exchange to work. WMNs are based on "trust-your neighbor" relationships. Also, the absence of fixed trust infrastructure,limited resources, connectivity andavailability,shared Wirelessmedium and physical vulnerability, make trust establishment virtually impossible.

Key Management :

All key-based cryptographic schemes demand a key management service, which is responsible for keeping track of bindings between keys and nodes and for securecommunication between nodes. Key distribution and key agreement over aninsecure channel are at high risk and suffer from potential attacks.

VII. CONCLUSIONS

In this paper, we have analyzed the constraints in the security of Wireless Mesh Networks. It is difficult to implement the security attributes due to the adhoc nature and power and computational constraints of the WMNs. The authentication of MRs is a critical issue. A secure multipath routing protocol is required. A distributed intrusion detection system is essential for monitoring the network continuously.

REFERENCES

1] Steve Glass, Marius PortmannandVallipuramMuthukkumarasamy, "Securing WirelessMesh Networks" -Queensland Research Lab, NICTA

2] ZeeshanFurqan, Shahabuddin Muhammad, "A Multi-agent Approach Toward the Security Analysis of the 802.11i Handshake Protocol" - School of Electrical Engineering and Computer Science, University of CentralFlorida, Orlando, Florida32816

3] Muhammad ShoaibSiddiqui, ChoongSeon Hong, "Security Issues in Wireless Mesh Networks",Department of Computer Engineering, KyungHeeUniversity.

4] NageshNandiraju, DeeptiNandiraju, LaksmiSanthanam, Bing He,Jungfang Wang,& Dharma P.Agarwal, "Wireless Mesh Networks: Current challenges and future directions of web in the sky", University of Cincinati, USA.