International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.405-418
http://dx.doi.org/10.14257/ijsia.2016.10.3.35

A Survey on Wireless Mesh Networks and its Security Issues

[1] R. Regan and [2] J. Martin Leo Manickam

[1] *Department of CSE, University College of Engineering, Villupuram, Anna University, India*
[2] *Department of ECE, St.Joseph's College of Engineering, Chennai, India*
[1]*reganr1985@gmail.com*,[2]*josephmartin_74@yahoo.co.in*

Abstract

Wireless Mesh Networks (WMNs) are have secured a significant position in the technological world due to their unique characteristics. These networks are dynamic, self-healing, and self-organizing in which the nodes reflexively set-up and maintain mesh connectivity with each other. Having these characteristics, WMNs enjoy great benefits such as low-upfront costs, reliability, and prompt troubleshooting. Despite all these fringe benefits, one of the greatest challenges in wireless mesh networks is that they are exposed to a number of hazardous security vulnerabilities. In this paper we investigate WMNs security attacks, security goals and various defense mechanisms for defending the attacks.

Keywords: *Wireless mesh network, Security attacks, Protection mechanisms*

1. Introduction

The Internet and wireless networks are heading towards finding out faster, simpler, and more efficient ways to get the users connected. WMNs are one of the key technologies to provide a solution in this perspective. These networks are dynamically self-organizing, self-healing, and self-configurable. They help to realize the future of network connectivity anywhere and anytime. These networks consist of two basic types of mesh networking nodes called mesh routers and mesh clients. These mesh clients not only function as hosts but also route information packets. Client nodes such as laptops, PDAs, and desktop PCs possessing wireless network interface card (NICs) can communicate directly with mesh routers to keep the users connected anywhere and anytime. In a WMN, mesh routers are usually static (or have minimum mobility) while mesh clients are either static or highly mobile. Mesh routers can be categorized into access, backbone, and gateway mesh routers. Mesh clients approach a mesh network through access mesh routers while the mesh backbone is connected to the Internet through gateway routers. These functionalities can coexist in a single router. Communication in a wireless mesh network is of multi-hop nature in which nodes behaving as routers forward packets on behalf of other nodes that are not in the direct transmission range of their destinations.

WMNs have many advantages other wireless networks. Deployment of WMNs is very easy. Wireless Mesh Networks (WMNs) are replacing wireless Infrastructure networks in many areas because of their lower cost and higher flexibility. Despite the benefits that can be achieved through wireless mesh networks, security is always a big concern to their users and administrators. Without a satisfactory level of security, users are reluctant and lack motivation to use services provided by WMNs. These networks cannot achieve distinguishable popularity and success in the technological world unless providing overwhelming security and reliable services to their users. Security schemes that have been developed for WLANs are not suitable enough to be incorporated in WMNs as there is no centralized trusted authority in WMNs to distribute the public key. Thus there is need of new security protocols and schemes should be developed for WMNs.

ISSN: 1738-9976 IJSIA

2. Wireless Mesh Networks Architecture

In terms of architecture and design, wireless mesh networks can generally be classified into three groups: infrastructure-less, infrastructure, and hybrid networks. These are briefly discussed in the following discussion.

.

2.1 Infrastructure-less / Client WMNs

Infrastructure-less mesh networks are one-tier networks in which client nodes participate in routing architecture and construct the real network. In addition to routing, network configuration functionality is also performed by these client nodes which eliminate the need of any special router. A wireless ad hoc network can be an example of infrastructure-less mesh networks [1].

2.2 Infrastructure/Backbone WMNs

In contrast to the infrastructure-less mesh, infrastructure mesh networks consist of a backbone of mesh routers and are two-tier networks. This backbone or infrastructure can be built using any of the various wireless radio technologies such as the IEEE 802.11. In these networks, mesh routers perform the routing functionalities and provide access to the users and clients. They behave as access points for the conventional clients. Usually, mesh routers in these networks use two levels of communication: backbone communication and user's communication.

2.3 Hybrid WMNs

Hybrid mesh networks provide combined functionalities of infrastructure and infrastructure-less networks. In addition to mesh routers, mesh clients also participate in routing by either connecting to a mesh router or by meshing with other mesh clients. This property of mesh clients enhances the coverage of the mesh backbone [2].

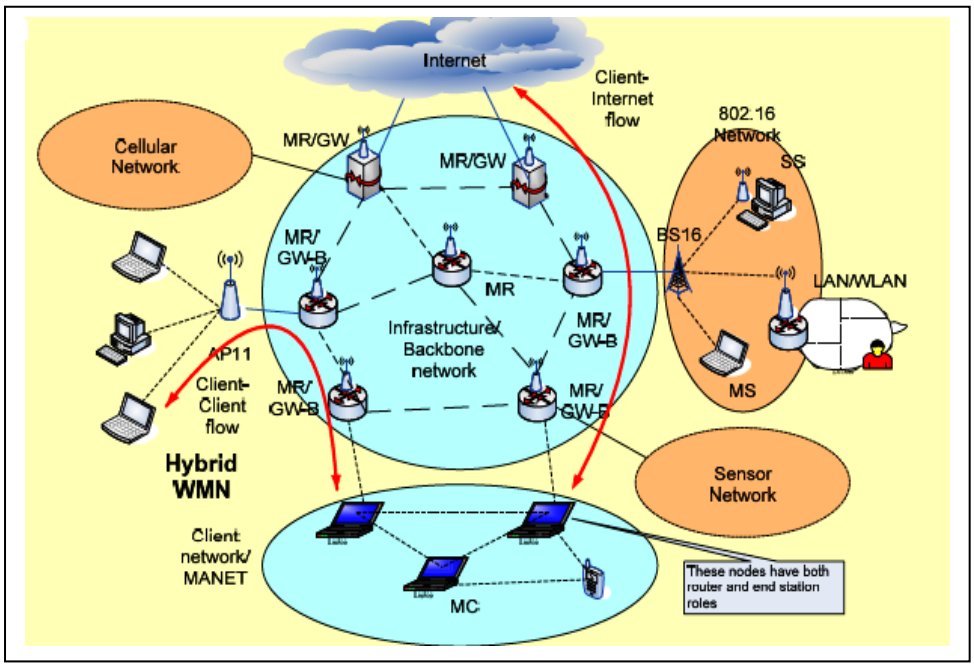

Figure 1.1. Hybrid WMN

3. Characteristics of WMNs

Wireless mesh networks are multi hop networks and provides much coverage range. Like if one node is failed or turns off then through other nodes message can be transmitted to destination nodes that function provides the redundancy in the mesh network. They have capability of self healing and self forming and self organization and provide support for Ad Hoc Networking. As we have multi-hoping so it achieves higher throughput, and more efficient frequency re-use. They provide low cost for installation because the reduction of the number of access points to internet so the main advantages of WMNs is that easiness of deployment. Multiple type of network access like support for internet and p2p communication as well. Provide compatibility with existing wireless networks like WiMax, Wi-Fi, cellular networks. It has flexible network architecture. [4]

4. Applications of WMNs

In order to prove the need and importance of WMNs, we now discuss some of the applications of these networks. A WMN can be deployed to render a wide variety of applications.

- **Building automation:** Different electrical devices such as fans, lights, and air conditioners etc. should be monitored in a building. Usually wired networks are used for this purpose which is of course expensive. The replacement of access points for building automation and control networks with mesh routers will reduce the cost and simplify the deployment.
- **Metropolitan area networks (MANs):** These networks might also be useful in MANs. It provides the higher transmission rate at the physical-layer as compare to other networks such as cellular networks. Like the transmission rate of IEEE 802.11g nodes is 54 Mbps. Economically it is a best alternative for underdeveloped regions and broadband networking.[3]
- **Enterprise networking:** This type of networking can be of any scale. It can be a small office, a medium-sized company within a building, or a large-scale network with multiple buildings. Replacing access points with mesh routers can eliminate the necessity of Ethernet wires. Moreover, WMNs can easily expand with the size of the enterprise.
- **Broadband home networking:** Similar to enterprise locations, broadband home networking is accomplished by using WLANs and the standard IEEE 802.11 protocols. Home networks using access points usually have zones with no coverage. Performing site surveys and installing multiple access points are expensive and impractical.
- **Community and neighborhood networking**: In most cases, the architecture used in communities for network access uses cable or DSL connected to the Internet and at the end-user's side a wireless router is connected to any of these two options. Accessing the network in this way raises many issues.
  - All traffic must flow through the Internet which reduces network resource utilization significantly.
  - Some areas in the neighborhood are not covered by wireless services.

  WMNs overcome all these limitations by providing flexible mesh connections between homes and communities [9].
- **Security surveillance systems:** To deploy surveillance systems at public and private premises such as company buildings, shopping malls, and grocery stores etc., WMN is a more feasible solution than wired network. Due to the frequent transfer of images and videos, these systems demand high network capacity which can be efficiently managed by WMNs.

.

All these applications demonstrate the importance of WMNs in the real world. While these networks provide great benefits to the society but because of their diverse application and properties, they also bring forth security vulnerabilities which lead to several kinds of severe attacks on these networks [5].

5. Security in Wireless Mesh Networks

Security issues and the potential of WMNs are cannot be ignored. Due to dynamic change of network topology, distributed network architecture and shared wireless mediums WMNs lacks in security solutions. Attacks can occur on different protocol layers which can harm the network traffic and data. In wireless mesh there are different types of architecture which may uses different approaches for wireless mesh security purpose [6].

5.1 Basic Prevention

The primary issues which are very necessary for privacy preventions are as follows:-

- **Data Confidentiality** Its main purpose to prevent from eavesdropping and protect the data against the attacks .It is controlled by intermediate mesh routers. The algorithm by which one can protect the data from misbehaviors is message encryption.

- **Traffic Confidentiality** Traffic confidentiality is quite difficult to prevent against the attacks. For traffic confidentiality users must know that to whom they are communicating and their traffic patterns must be followed by the communicators. It is usually occurred by the attackers at mesh routers while traffic transfer. By following the key distribution mechanism WMNs can overcome on this type of attacks. [7]

5.2 Mesh Security

802.11s is a standard which will be followed in future for all kind of commercial mesh products. Right now mesh products are using different approaches for security and many of them may be derived from existing ad-hoc security mechanisms. 802.11s is a standard which will be based primarily on 802.11i security mechanisms.

5.2.1 Confidentiality

In this the whole path should be protected and message should not be altered during the communication. Users must know each other for secure communication. The message and data information should not be disclosed. The data is only revealed to the intentional users in order to maintain the confidentiality of some classified information. Routing information must remain confidential as the information might be valuable for enemies to identify and locate their targets in a battlefield in some cases.

5.2.2 Availability

Insurance of authorized user actions can be done for secure communication. Provide the reliable delivery of data to the destination node. Protect the message and data against DoS (Denial of Service). This security requirement is challenged mainly during the 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. A DoS attack could be launched at any layer of the network [8].

5.2.3 Authentication

In WMNs authentication is very important because of change of shared medium. Authenticity is essentially assurance that participants in communication are genuine and not impersonators. A proper mechanism should be followed for data sending and receiving. Users must know each other because it very necessary for reliable transmission of data. Without the use of an authentication mechanism, the adversary could impersonate a benign entity and thus gain access to confidential resources.

5.2.4 Authorization

Users have the right to amend the data. If anybody wants to perform any task then there should be a proper process which ensures that the person have right to perform that task. 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.

5.2.5 Integrity

Integrity guarantees that a message being transferred will never corrupt. Integrity can be compromised mainly in the following two important ways [10]:

- **Malicious altering** - such as an attacker altering an account number in a bank transaction
- **Accidental altering** - such as a transmission error.

5.2.6 Access Control

User should ensure that only authorized actions can be performed, like if one cannot have authorization of changing the message then that user must be communicate with administrator for performing that task which he/she wants to perform.

5.2.7 Non-repudiation

It ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. Non-repudiation is useful for detection and isolation of a node with some abnormal behavior. For instance, when node-A receives an incorrect message from node-B, non-repudiation allows node-A to accuse node-B using this message and to convince other nodes that node-B is compromised.

6. Vulnerabilities and Attacks in WMNs

Security in wireless networks can be of two types: information security and network security. Security attacks in WMNs can generally be categorized into two classes: passive and active attacks. Here we briefly explain the most common types of security attacks that can jeopardize any WMN [11, 12]

6.1 Passive Attacks

Attackers in passive attacks are usually hidden and try to tap in the communication channels to get unauthorized data access. In these attacks, the adversaries, rather than actively injecting or manipulating information, just listen to the communication of benign nodes for their own benefits. These types of attacks are usually against data confidentiality. Examples of passive attacks are passive eavesdropping and traffic analysis.

6.1.1 Passive Eavesdropping

This attack is successful when communication between benign nodes is in plain text. Unencrypted data can be easily eavesdropped by tapping the wireless communication. For example, an adversary can tap information about credit cards, passwords, and other confidential data while this information is being transmitted over a wireless link.

6.1.2 Traffic Analysis

In addition to the contents of data packets, the traffic owing pattern can also be beneficial for the adversary. The traffic analysis can be done using the following techniques:

- The carrier is sensed at the physical layer and a particular node is observed for its incoming and outgoing traffic.
- The headers of frames can be analyzed for routing details and topology of the network.
- Transmission of packets by a node can be correlated to find the routing path in addition to the source and destination nodes.
- In a clustered environment, analyzing the traffic of a cluster coordinator (cluster head) might be useful for the adversary.[9]

6.2 Active Attacks

In addition to passive attacks, adversaries can execute even worse type of attacks categorized as active attacks. In these attacks, the adversary manipulates the communication or operation in the network by forging, altering, blocking, or re-routing messages. Active attacks not only compromise data confidentiality, but also affect data integrity. Active attacks can be broadly categorized into four types:

6.2.1 Physical Attacks

This includes damage to hardware, electromagnetic pulse attacks, and micro-probing etc. Physical attacks against hardware can be a serious issue. When nodes are unattended and can be physically reached by the adversary, tampering techniques such as micro-probing, laser cutting, focused ion-beam manipulation, glitch attacks, and power analysis can be used to attack the hardware [13]. This tampering can also help in masquerading and attacks.

6.2.2 Misbehaviors

Nodes may show selfishness to gain unfair shares of resources or deny to pay for charged services. Salem et al. [14] discuss various attacks against the charging schemes in multi-hop networks providing these services:

- **Dishonesty**: In multi-hop networks, intermediate nodes are required to relay the packets to others. Rewarding mechanisms such as `paying' can be designed in this regard. A dishonest node may try to prove that it was involved in the forwarding but actually it is not.
- **Denial of usage:** A node may refuse that it has carried out any communication mentioned on the payment bill.
- **Piggybacking:** Intermediate nodes on the route between a source and a destination may piggyback their own packets on to the ongoing communication to avert bill payment.

6.2.3 Unauthorized Access

When a node starts communicating in a WMN, it first needs to be authenticated and authorized to join and use services of the network. If the authorization and authentication mechanisms fail in the process, any unauthorized node can get access to the network.

6.2.4 Message Forgery and Replay Attacks

Attackers can modify the actual message contents maliciously or resend the acknowledged message. These attacks manipulate the message integrity. Adversaries can inject forged messages into the network, resulting the network protocols to malfunction.

6.2.5 Man-in-the-middle Attack

An adversary can try to reside between mesh clients and mesh routers or two mesh routers to intercept and manipulate their communication. For example, an adversary can set up a rogue mesh router to induce other routers or clients to communicate with it. This vital attack can compromise both information and network security and can affect any type of nodes (routers or clients).

6.2.6 Sleep Deprivation and Packet Dropping Attacks

An attacker may drain the battery of victim notes which will ultimately destroy the computational power of the victim node. If a node is not relaying the packets then packet dropping attack can also be occurred.

6.2.7 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. Security mechanism of impersonation attacks could be to apply strong authentication methods in contexts where a party has to be able to trust the origin of data it has received or stored.

6.2.8 Denial of Service

A denial of service (DoS) or distributed denial of service (DDoS) attack affects the availability of the network services or simply partitions the network[15]. It decreases a network's ability to perform accurately according to its anticipated capacity in a timely manner. DoS attacks could happen at all the layers in the protocol stack from the physical to the application layer. Some well-known examples of DoS attacks at different protocol layers are channel jamming, wormhole attack, fooding, Sybil attack, black hole, and gray hole attacks. Here we briefly define some of these attacks

- **Flooding Attack and Jamming Attacks**: An attacker can send a MAC control messages to its neighbor users so due to that neighbor can suffer with the DoS problem. It can also affect the victim node’s battery and channel bandwidth. Jamming Attacks may affect the performance of wireless networks. To overcome on this type of attack one can use RTS signal jamming. This is also known as DoS on the victim nodes.
- **Wormholes Attacks (WHA):** WHA can be severely problematic. 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 are 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[16].

- **Black hole attack and Gray whole attack:** An adversarial node may drop all packets it is supposed to forward to other nodes. A successful attack may block all the communication around the victimized node. Gray whole attack: A malicious node may drop selected packets from the received packets and forward all the others. This makes it difficult to be detected. This attack is also called selective forwarding attack.
- **Sybil attacks:** A type of attacks where a node creates multiple illegitimate identities in sensor networks either by stealing or fabricating the identities of legitimate nodes. It can be used against topology maintenance and routing algorithms another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

6.2.9 Routing Attack

There are many attacks which can harm the routing tables and disturb the route traffic. Followings are the unique attacks which can come in wireless mesh networks:-

- **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.

Thus the routing mechanisms of WMN must be secured. The usual mechanism, to ensure integrity of data, is using hash functions and message digest [17].

7. Related Work

V.S .Shankar Sriram [18] proposed architecture and analyzed the possibility of wormhole attack along with a countermeasure to avoid such an attack. The proposed work involves the shared information between communicating access points to prevent Rouge Access Points from masquerading as false neighbours. The author's defense greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization. As initial research focused that wormhole attack is possible only on adhoc networks, but now-a-days wormhole attack is possible on infrastructure based wireless LANs also.

Shin-Ming Cheng [19] proposed the Combined Distributed and Centralized scheme (CDC) to combine the distributed scheduling and centralized scheduling mechanisms so that the mini slot allocation can be more flexible, and the utilization is increased. In the 802.16 mesh mode, allocation of mini slots can be handled by the centralized and distributed scheduling mechanisms. For the centralized scheduling mechanism - two scheduling algorithms named

Round Robin (RR) and Greedy, are proposed as the baseline algorithms.

Divya Bansal [20] proposed a new approach using threshold authorization model with Clustered Certificate Authority which caters to the best of both the centralized and distributed architecture. As various wireless networks evolve into the next generation to

provide good services, a key technology, wireless mesh networks (WMNs), has emerged recently. There are number of issues in the deployment of WMNs. Security is quite a serious issue amongst them. Authenticating the users and devices is a key point of network security in the network.

P Subhash and S Ramchandram[21] proposed a mechanism to prevent byzantine wormhole attack in WMNs. The proposed work relies on digital signatures and prevents formation of wormholes during route discovery process and it is designed for an on-demand hop-by-hop routing protocol like HWMP (Hybrid Wireless Mesh Protocol-the default routing protocol for WMN). This is also applicable to source routing protocols like DSR (Dynamic Source Routing). This is a software based solution and does not require additional (or) specialized hardware.

Monika [22] studied to mesh routers which are stationary and implemented both Gray Hole attack and black hole attack in mesh routers and study the delivery ratio of the network with and without the presence of attack routers. DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet accesses this type of attacks are common in the network. Wireless mesh networks consist of both mesh routers and mesh clients.

Mohammad N. Al-Mohidat and Fathi M. Salem [23], proposed an effective modification to the IEEE 802.11 MAC(Medium Access Control) layer by incorporating a multi-channel mode and shows significant improvement in many major network performance metrics compared to the literature and to the single channel mode. As the multi-hop nature of WMNs creates many new challenges, primarily in the MAC layer and specifically, the IEEE 802.11 Medium Access Control (MAC) layer is designed for a single hop wireless network.

Huaiyu Wen and Guangchun Luo [24] proposed a high efficiency wormhole detection algorithm based on 2-hop neighbor in WMNs, which is called Wormhole Detection based on Neighbour's Neighbour scheme (WDNN) to enhance the efficiency and facility of wormhole detection .Then a simple Random Walk Route scheme (RWR) is proposed to prevent routes from wormholes in which the route is chosen without using the low latency link which is created by wormholes.

Lim et al. [26] propose an intrusion detection system for wireless networks that consists of a number of devices deployed throughout the network. The IDS works at different level. At the basic level, it carries out a MAC address filtering if it cannot find the MAC address of a device in the white-list. For intrusion response, the system uses ARP poisoning and a disassociation-reassociation strategy with the suspected node. However, the proposed intrusion response mechanisms are computationally expensive and their invocation may adversely affect network performance.

Konorski and Kurant have proposed a protocol called R-hash to prevent MAC layer misbehavior [27].The scheme intends to prevent MAC layer misbehavior of nodes by using a hash function-based mechanism. The winner of a contention for accessing the wireless channel is determined by using a public hash function to the feedback that each station gets from the contention. This strategy effectively confuses a potential misbehaving station so that no possible modification can be made on the probability distribution of transmission delay for the contending stations.

A proposition based on game theory for handling misbehavior in the MAC is been presented by Cagalj et al. [28]. The optimum strategy for each node has been derived in terms of controlling the cannel access probability by adjusting the contention window, so that the equilibrium point is reached in the overall network. The authors have also derived conditions under which the Nash equilibrium of the network is Pareto optimal for each node in the network as well, when some of the nodes in the network are misbehaving.

Mishra and Arbaugh propose a standard mechanism for client authentication and access control to guarantee a high-level of flexibility and transparency to all users in a wireless network [29]. The users can access the mesh network without requiring any change in their devices and softwares. However, client mobility can pose severe problems to the security architecture, especially when real-time traffic is transmitted.

Prasad et al. have presented a lightweight authentication, authorization and accounting (AAA)infrastructure for providing continuous, on-demand, end-to-end security in heterogeneous networks including WMNs [30]. The notion of a security manager is used by deploying an AAA broker. The broker acts as a settlement agent, providing security and a central point of contact for many service providers.

Pirzada and McDonald propose an approach to building trust among the nodes in an ad hoc network that can be deployed in a WMN which does not have a centralized trusted entity [31]. In this scheme, the nodes passively monitor the packets received and forwarded by their neighbors. The receiving and forwarding of packets are considered as events. The events are assigned different weights based on the applications and the forwarding behaviors of the nodes. The weights reflect the significance of the concerned event with respect to the associated applications. The trust values associated with all the events of a node are combined to arrive at an aggregate trust metric for the node. The computed trustvalues of a pair of nodes are used for deriving the trust value of the link connecting those nodes. The links which have higher trusted values are assigned smaller weights and a shortest-path algorithm is utilized to find the most trusted path (i.e., the path with the minimum weight) between a pair of nodes.

Martignon et al. have presented a security architecture MobiSEC that provides access control in a WMN [25].It is an efficient scheme for secure authentication and access control in WMNs. It proposes a two-step approach for authentication of an mesh clients (MC) with its mesh routers **(**MR). In the first step, the MC authenticates to the nearest MR. In the second phase, the MC uses a protocol that is based on the transport layer security and uses a certificate issued by a CA with the AAA server to additionally authenticate as a router. The key distribution may be server driven or client driven. In the server driven, each MR contacts a key distribution server for getting the key list, while in the client driven protocol, the MR obtains a seed from the server and a hash function to generate the key. The mobility of the MRs in the backbone is facilitated by having each router using the same key for authentication. The protocol addresses access control issues including authentication and key establishment. However, it does not address issues like message confidentiality, message integrity, and protection against replay attacks.

Sen and Subramanyam have proposed and evaluated the performance of a distributed certificate authority based on threshold cryptography [33]. The scheme is an extension of the MOCA protocol [34] in which a collection of nodes selected on several parameters acts as the certificate authority and provides an attack resilient and robust certificate distribution and verification service.

Lin et al. have proposed a two-factor localized authentication scheme for inter-domain handover and mobility management in IEEE 802.11 standard compliant WMNs [32] .It utilizes the asymmetric property of Rabin cryptosystem in mobility management issues where APs have high computational power and the MSs are resource-constrained. For providing enhanced security, it uses two-factor authentication for roaming mobile users. The scheme is resistant to attacks such as: replay, impersonation, password guessing and attack on the privacy of the users.

8. Conclusion

WMNs have become an important focus area of research in recent years owing to their great promise in realizing numerous next-generation wireless services. However, the property of being a multi-hop network with intermediate relay nodes puts the level of

security in these networks into high risk. Moreover, the absence of a centralized trusted mechanism can also jeopardize the security of these networks. Hence, these networks become extremely vulnerable to intense information disclosure and network misuse attacks such as eavesdropping, man-in-the-middle attacks, and DoS attacks. In addition, malicious nodes or users might also become a threat. It is therefore required to have an efficient protection mechanism that can mitigate the severity of these attacks and provide seamless authentication scheme with least possible overhead. However, if these security issues are efficiently handled, these networks have the ability to provide multiple services to their users concurrently such as online banking, community based file sharing, and live video streaming etc. Thus this survey presents various security issues and challenges in WMN, describe the major security requirements for the wireless mesh network and protection mechanisms to the security issues in the WMN are analyzed.

References

[1] I. F. Akyildiz, X. Wang and W. Wang, "Wireless mesh networks:A survey", Computer Networks, IEEE , **(2005)**, pp. 445-487.
[2] E. Borcoci, "Wireless Mesh Networks Technologies:Architectures, Protocols, Resource Management and Applications", INFOWARE Conference; Cannes, France.
[3] I. Akyildiz and X. Wang, "Wireless Mesh Networks (Advanced Texts in Communications and Networking)", John Wiley & Sons, **(2009)**.
[4] M. S. Siddiqui and C. S. Hong, "Security Issues in Wireless Mesh Networks", IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE), **(2007)**.
[5] Z. Hamid and S. A. Khan, "An Augmented Security Protocol for Wireless MAN Mesh Networks", Communications and Information Technologies, ISCIT International Symposium, **(2006)**.
[6] A. Gerkis, "A Survey of Wireless Mesh Networking Security Technology and Threats", **(2006)**.
[7] I. F. Akyildiz and X. Wang, "Security in Wireless Mesh Networks", **(2006)**.
[8] X. Gu and R. Hunt, "Wireless LAN Attacks and Vulnerabilities", Proceeding of IASTED Networks and Communication Systems, **(2005)**.
[9] M. S. Fahad and S. Karachi, "Securing Wireless Mesh Networks a Three Dimensional Perspective", Mittwoch, **(2011)**.
[10] H. Redwan and K.-H. Kim,"Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", IEEE Xplore, **(2008)**.
[11] I. Akyildiz and X. Wang, "Wireless Mesh Networks (Advanced Texts in Communications and Networking)", John Wiley & Sons, **(2009)**.
[12] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", Wiley, **(2009)**.
[13] O. Kommerling and M. G. Kuhn, "Design principles for tamper resistant smartcard processors", Proceedings of the USENIX Work-shop on Smartcard Technology, USENIX Association, **(1999)**, pp. 2-2.
[14] N. B. Salem, L. Butty_An, J.-P. Hubaux and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multihopcellular networks", Proceedings of the 4th ACM International Symposium on Mobile Ad hoc Networking and Computing, MobiHoc, ACM, **(2003)**.
[15] Monika Department of computer science, "Denial of Service Attacks in Wireless Mesh Networks", International Journal of Computer Science and Information Technologies, vol. 3, no. 3, **(2012)**, pp. 4516-4522.
[16] V. S. S. Sriram, A. P. Singh and G. Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, no. 1, vol. 1, **(2009)**.
[17] S. D. Kanawat and P. S. Parihar, "Attacks in Wireless Networks", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), vol. 1, no. 1, **(2011)**.
[18] V. S. S. Sriram, A. P. Singh and G. Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, vol. 1, no. 1, **(2009)**.
[19] S.-M. Cheng, P. Lin, D.-W. Huang and S.-R. Yang, "A Study on Distributed/Centralized Scheduling for Wireless Mesh Networks", IWCMC'06, July 3–6, pp 599-604, 2006, Vancouver, British Columbia, Canada
[20] D. Bansal and S. Sofat, "Threshold based Authorization model for Authentication of a node in Wireless Mesh Networks", Int. Journal of Advanced Networking and Applications, vol. 1, no. 6, **(2010)**, pp. 387-392.
[21] P. Subhash and S. Ramachandram, "Preventing Wormholes in Multihop Wireless Mesh Networks",Third International Conference on Advanced Computing & Communication Technologies, IEEE, **(2013)**.

[22] Monika Department of computer science, "Denial of Service Attacks in Wireless Mesh Networks", International Journal of Computer Science and Information Technologies, vol. 3, no. 3, **(2012)**, pp. 4516- 4522.
[23] M. N. Al-Mohidat and F. M. Salem, "IEEE 802.11 Based Wireless Mesh Networks: A Multi-Channel MAC Baseline Study", IEEE, **(2013)**.
[24] H. Wen and G. Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbour in Wireless Mesh Networks", Journal of Information & Computational Science, vol. 10,14, **(2013)**, pp. 4461–4476.
[25] J. Sen, "Security and Privacy Issues in Wireless Mesh. Networks: A Survey", Innovation Labs, Tata Consultancy Services Ltd., **(2013)**.
[26] Y.-X. Lim, T. S. Yer, J. Levine and H. L. Owen, "Wireless intrusion detection and response", Proceedings of Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, **(2003)**; West Point, NY, USA..
[27] J. Konorski and M. Kurant, "Application of a hash function to discourage MAC-layer misbehaviour in wireless LANS", Journal of Telecommunications and Information Technology, vol. 2, **(2004)**, pp. 38-46.
[28] M. Cagalj, S. Ganeriwal, I. Aad and J.-P. Hubaux, "On cheating in CSMA/CA ad hoc networks", Technical Report IC/2004/27, EPFL-DI-ICA, **(2004)**.
[29] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard", Technical Report CS-TR-4328, Computer Science Department, University of Maryland, USA, **(2002)**.
[30] N. R. Prasad, M. Alam and M. Ruggieri, "Light-weight AAA infrastructure for mobility support across heterogeneous networks", Wireless Personal Communications, vol. 29, no. 3 - 4, **(2004)**, pp. 205–219.
[31] A. Pirzada and C. McDonald, "Establishing trust in pure ad hoc networks", Proceedings of the 27th Australian Conference on Computer Science, **(2004)**; Dunedin, New Zealand.
[32] X. Lin, X. Ling, H. Zhu, P.-H. Ho and X. S. Shen, "A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks", International Journal of Security and Networks, vol. 3, no. 2, **(2008)**, pp. 122-132.
[33] J. Sen and H. Subramanyam, "An efficient certificate authority for ad hoc networks", Proceedings of the 4th International Conference on Distributed Computing and Internet Technology (ICDCIT), Bangalore, India, Lecture Notes in Computer Science, Springer-Verlag, **(2007)**; Germany.
[34] S. Yi and R. Kravets, "MOCA: mobile certificate authority for wireless ad hoc networks", Proceedings of the 2nd Annual PKI Research Workshop Program (PKI), Gaithersburg, **(2003)**; Maryland.

Authors

R.Regan, He is working as an Assistant Professor in the department of Computer Science and Engineering at University College of Engineering Villupuram, Anna University, India . He acquired B.E. Degree in Electronics and Communication Engineering from Mailam Engineering College, Mailam in 2006. He received M.Tech Degree in Computer Science and Engineering from Bharath University, Chennai in 2010. He is pursuing Ph.D Degree in the Faculty of Information and Communication Engineering at Anna University, Chennai. He has over 5 years of experience in educational institution. He has to his credit 10 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Wireless security.

J. Martin Leo Manickam, He is working as Professor in the Department Electronics and Communication Engineering at St. Joseph's College of Engineering, Chennai. He acquired B.E. Degree in Electronics and Communication Engineering from Alagappa Chettiar College of Engineering and Technology, Karaikkudi in 1995. He received M.E. Degree in Optical Communication and Ph.D degree in the Faculty of Information and communication Engineering from the College of Engineering, Anna University, Chennai. He has over 16 years of experience in teaching and guiding projects for

Undergraduate and post graduate students. Under his guidance, One scholar had got Ph.D degree and 12 research scholars are pursuing their Ph.D programme. He has to his credit 15 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Digital Communication and Network Security.