SECURITY CONCERN IN WIRELESS MESH NETWORKS

Satendra (M.Tech)
Monad University-Hapur, Uttar Pradesh
+91-7835963704

Abstract

WMN, the Wireless Mesh Network does not rely on permanent infrastructure. Wireless internet service suppliers are deciding WMNs to suggest internet connectivity, as it permits a fast, easy and inexpensive deployment network. WMN is a self organized and self configured network. It means that nodes in mesh network design automatically established and maintain network connectivity. In such types of network security is an important issue. This paper describes the security issues and challenges in WMN

Keywords

Wireless Mesh Network (WMN), Architecture, Security, Issues and Challenges.

1 Introduction

WMN are Ad hoc Wireless Network that are formed to provide an alternate communication infrastructure for mobile or fixed node without the spectrum reuse constraints and the required of network planning of cellular network. The mesh topology provides many alternate paths to transmit the data session between sources to destination; each user may easily send data to source to destination. At the time of data transfers if any nodes are failure to transmit the data then it Reconfiguration the path among source to destination. In generally mesh nodes are used to transferring the data for the WMN network. WMN is a self organized and self configured. It means that nodes in mesh network design is automatically establish and maintain network connectivity [1]. They can provide the each other to distribute the data connectivity from mesh nodes to user through the responsible nodes and internet gateways. The many advantages of WMN like multiple interfaces, increased reliability, multiple radio frequencies, low Deployment cost, self organization and self configuration.

WMN is an application of ad hoc network and the operation of WMN is similar to Mobile ad hoc Network (MANET). WMN is shows as potential wireless technology for a number of promising and commercially interesting applications such as broadband home networking, community, coordinate network management, mobile application, military operations, health care, industrial application, intelligent transportation system, hospitality and Broadband Wireless Access.

The rest of the paper is as follows. In Section 2 explain an overview of related work. Section3 describe the taxonomy of WMN. Section 4 starts with a description of the security Model for the considered architecture of WMN and discuss the requirement of security mechanisms in Section 5.we can discuss also the benefits, issues and challenges of WMN in Section 6 and Section 7. Finally Section 8 explains the conclusion.

2 Related Work

About the previous years, a number of security architectures and method have been devised for Wireless Mesh Networks (WMNs). In WMN a number of parameter are used for security like authentication, integrity, confidentiality, availability and threats etc. In the past used the ring topology but time is changed we can used the mesh topology. For example, [2] proposed ARSA for provide security architecture. In which the user can access the data and send to third party. It can solve the problem of pair-wise trust between operative of the different WMN. Study about DoS attacks in which enemy generate an overflow of high-rate data flows to reject service to other. So it can study about different types of attacks through choosy random sinking [3]. The author proposed PEACE. Schemes in which PEACE provides the security solution through authentication and it also provides protection through attacks [4]. In [5] suggests the three generation mobile network architecture in wireless back hauls for security issues. How to provide the security issues to our mobile network. So author described the security model and architecture for mobile network. Author extends the 3gpp model for WMB network contain the some security issues like confidentiality, integrity, authentication, non-reputation, availability and privacy used between the source and destination for security solution So the main motive of paper to resolve the security issues in mobile network. Many protocol protect at only single protocol layer not other layer. So author suggest a security analysis inherit to another network. We know that the WMN and WSN both have same advantages like energy efficient, power consumption, low memory etc. There are different types of attacks like confidentiality attacks, integrity attacks and identity attack. Author suggests resolving the problem by using intrusion detection i.e. orthogonal to network protocol. It based on reputation system and self organization maps (unsupervised learning). It can use the security technology of wireless Sensor Network (WSN) in WMN [7]. We combine the reputation with SOM it detects with distributed attacks. So it can resolve the routing behavior and resource utilization in WMN. Wireless Local Area Network (WLAN) is a part of WMN security system. WMN to provide encryption, authentication and access control between mesh (wireless)node and Access point (AP) in WMN. WMN architecture provides the security in infrastructure and infrastructure less. Security mechanism provides the security in Ad hoc network and MANET [6]. Sen. [8] provides the label switching technique to promote data traffic during the network from source to destination. It can provide the secure paths designed for data traffic transmission. O.E. Muogilim at el. [9] proposed Traffic Engineering (TE) for WMN. It can resolve the security problem WMN likes data traffic, traffic load, delay ratio, increase bandwidth and integrity, in TE three types of security mechanism are used like multiple protocol LAN Switching Traffic Engineering (MPLS-TE), like multiple protocol LAN switching Virtual packet network (MPLS VPN) and like Multiple protocol LAN Switching Virtual packet Network Internet protocol (MPLS VPN IPSEC). So author proposed VPN IPSEC for security threats in WMN. It is better as compare to MPLS-TE and MPLS VPN. So VPN IPSEC provides the security like encryption, tunneling, cryptography and authentication. The purpose of this paper described the detailed of network security requirement in WMN. So rest of the described the requirement of security, taxonomy, benefit and issues and challenges of WMN

3 TAXONOMY OF WMN

The taxonomy of WMN is described the brief idea of the paper. In (Figure 1) WMN is classified based on connectivity of various network types like Point-To-Point (PTP), point-To-Multiple (PTM) and Multipoint-To-Multipoint (MTM) [10].

3.1 PTP

In which all signal are transmitted between sources to destination. User can send the data from point-to-point. It can provide high performance, high speed interconnections between nodes. In which two nodes easily communicate to each others. It can easily deploy.

3.2 PTM

In which user have more than one connection to single nodes. The multiple nodes are used to establish a connection between source and destination. It is classified into two types are infrastructure based and less infrastructure.

3.3 MTM

MTM wireless networks use multiple hops to increase coverage without the need for raising the communication power it can provide the high reliability, flexibility and scalability to contain a large number of users.

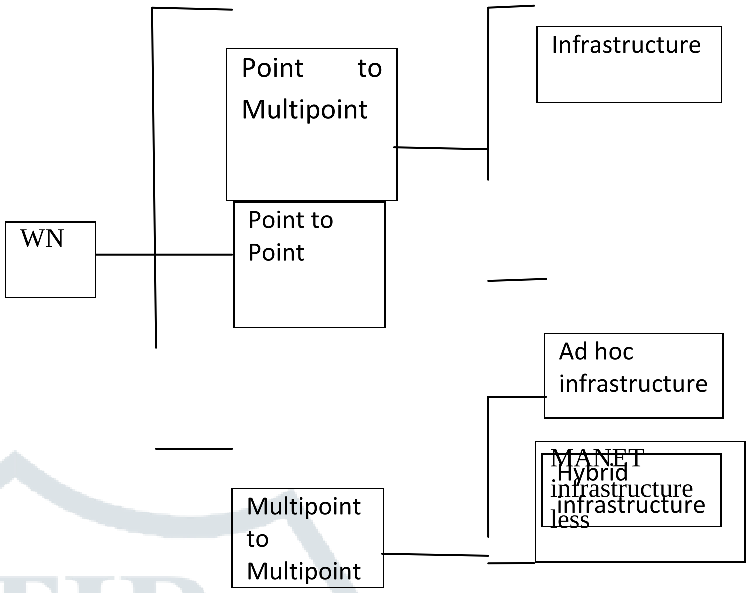

Figure 1: Taxonomy of WMN

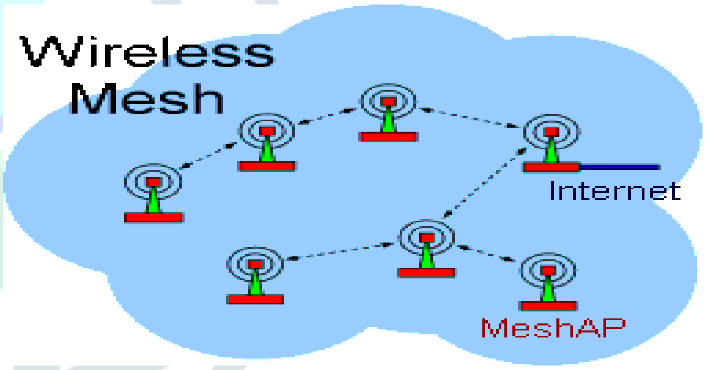

Figure 2: Wireless Mesh Network

4 WMN ARCHITECTURE

In the architecture of WMN (see Figure 2), it is consists of three types of nodes are Mesh client, Mesh router and Mesh backbone. Mesh client are end users devices like laptops, mobile phones etc. It can access the network by using such applications like email, game and location detection etc. The two level of nodes operation are used in Mesh client. At peripherals and on the access point (AP) and Mesh router are fixed or minimum mobility and it is used to direct data traffic from source to destination [11].

The AP provides the integration between the mesh client and mesh backbone infrastructure in WMN. WMN is a self organized and self configured. The excellent feature of WMN is to access the wireless technology for multimedia.

5 SECURITY REQUIREMENTS

The several security requirements are important of many applications. Some security requirements are described in table 1:

- Confidentiality
- Authentication
- Non-Reputation
- Privacy
- Integrity

Table 1: security requirement [12]

Security Requirement	Description
Confidentiality	Message must encrypt at sender site and decrypted at receiver site.
Authentication	Provide service beyond on integrity.
Integrity	It means that receiver received the data from user. No data change at the time of transmission.
Non-Reputation	The user can send the data from source to destination, and then user have proof that data transmission is send.

6 BENEFITS

WMN is a complete solution for covering large areas of coverage large areas of coverage. It is deal to deliver high throughput and highly reliable wireless connectivity. WMN is like a grid technology, in which wireless mesh node communicate with other nodes without routed from side to side reduce. WMN is a self healing, self organized and self learning. Due to this technology all the impossible problems to be possible easily like wireless connectivity between cities with inexpensive technology. Without any wired user can access the data at anytime and anywhere like campus, colleges, industries, Health care. WMN shows as potential wireless technology for a number of promising and commercially interesting application such as mobile application, broadband, home networking, network management, military operation, industries application etc [13].

7 ISSUES AND CHALLENGES

WMN is becomes very popular in wireless networking technology for create the network connectivity for home networking, community etc. It is necessary to efficient design and secure communication protocol for the WMN. The several parameter are used in the field of security like detect threats, black hole, colluding miserly, authentication, DOS attacks etc.

The various security challenges related to WMN like firstly, WMN level to active attacks, Passive attacks and message distortion. The active and passive attacks like integrity, authentication, availability, non-repudiation and confidentiality. Secondly, we know that WMN is dynamic self organization and self configured. It means that all nodes in mesh network design is authenticate established and maintain network connection [4]. Some security attacks and research issues are described in Table 2.

7.1 Physical Layer

The challenges of physical layer are not different to other technology. In WMN, the physical layer should be Reliable. At the Radio transmission, several spread spectrum like Code Division Multiple Access (CDMA), Frequency Hopping Spread Spectrum (FHSS), and Orthogonal Frequency Division Multiplexing (OFDM) and Ultra-Wide Band (UWB) increase reliability. So it can accomplish much better spectrum utilization and feasible frequency planning for WMN. The common folds issues in physical layer are: Firstly, it is necessary to more recover the transmission rate performance at physical layer technique. According to the scope of multiple antenna system have been reached Secondly, it can provide the advanced higher features provided by higher layer protocol. Physical layer, and MAC layer. It can makes hardware design more challenging [15].

7.2 Data link Layer

Data link layer (DLL) is second layer, in which to access and transmission in the radio channel. The many attacks are found in DLL like traffic flooding, collision, rate limitation is resolved by Enhanced Distributed Channel Access (EDCA). In which author proposed the QOS function this layer is main design for MAC protocol. The multiple MAC protocol means to receive the data from more than one channel for one user transmission. So it can increase the overall performance and MAC layer for smart antenna part for 3G. The advantage of smarter MAC layer are increase link budget, reduced transmission power, increase reliability, layer transmission range. The different types of antenna at DLL are: passive eavesdropping, MAC address spoofing, jamming, replay, unfairness in allocation and partial matching. Following issues at DLL WMN are scalable Mac, MAC physical Cross Layer Design and network integration in Mac layer.

7.3 Network Layer

In generally the main function of network layer is transfer the packet from source to destination during multiple hops. According to these respect, WMN is different from MANET, Ad hoc network and 3G systems. In any technology routing protocol is very important factor but in WMN it is different

between failure and success. [15]. The different types of routing protocol are multipath routing, Multi radio routing, Hierarchical Routing, and Geographic Routing. The main issues at Network Layer are as follows: better performance, scalability, Efficiency.
The two types of attacks in network layer: Control packet Attacks and Data packet Attacks. Both these attacks could be either in active or passive. Rushing attacks, wormhole attack, Black hole attack, Sybill attacks are found in Control Packet Attack. Passive eavesdropping attacks found in data packet.

7.4 Transport Layer

According to previous knowledge no protocol has been planned in particular WMN. Transport protocols are available for ad hoc networks. Such as different type of attacks are: SYN flooding attack, Desynchronized attack and Session Hijacking attacks. The open issues are to resolved the cross Layer solution network asymmetry and adaptive TCP.

Table 2: Security attacks and research issues in WMN protocol layer

Layer	Responsibility	Attacks	Research issues
Physical layer	Frequency, Carrier frequency generation, Modulation data encryption.	Jamming attack	It improves the transmission rates and utilization of advanced feature.
Data link layer	One hop communication	Passive , Jamming, MAC address spoofing, Replay, Precomputation and partial matching	Scalable MAC, network integration in MAC layer
Network layer	Transfer the packet from source to destination at multiple hop	Control packet and data packet attacks	Scalability, Efficiency
Transport layer	Authentication. EAP	SYN flooding and Resynchronization attacks	Adaptive TCP, Adaptive rate control
Application layer	Antivirus, Application Authentication	Repudiation, data corruption-n, logic layer	Improve exist application layer protocol and internet access

7.5 Application Layer

At the Application Layer, it requires a complete knowledge of the communicating applications as well as concession all the lower layer, the many applications are supported by WMN storage and sharing, information exchange across multiple wireless networks. The following attacks are found at application like Flooding attacks, Snooping attacks, Malwares, viruses and worms.

8 CONCLUSIONS

WMN is a self healing, self organized and self learning network. There are many advantage of WMN like multiple interface, increased reliability, multiple radio frequencies , low deployment cost, self organization and self configuration but there are also some security challenges and issues. This paper discusses the security requirements, threat, challenges and issues of WMN. Now WMN technology facing multiple problems related to security which requires the consideration in the development of efficient wireless network.

REFERENCE

[1] Johnston D, Walker J.2004. Overview of IEEE 802.16 Security. IEEE Security and Privacy: 2(3): 40-8.

[2] Zhang Y, Fang Y. ARSA.2006. An attack- resilient security architecture for multi-hop wireless mesh network. IEEE journal on selected Areas in communications: 24(10): 1916-28.

[3] Yan Y, Cao J, Li Z. 2009. Stochastic security performance of active cache based defense against dos attacks in wireless mesh network. In: Second International Conference on Advances in mesh networks (MESH 2009): P P: 30-6.

[4] Ren K, Yu S, Lou W, Zhang Y.2010. PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks. IEEE Transactions on parallel an Distributed Systems: 21(2):203-15.

[5] Frank A, Z, Sebastian R, Albert B.2011.Security analysis of wireless mesh backhauls for mobile networks, Journal of Network and Computer Applications. Elsevier, 432-442.

[6] Kuhlman D, Moriarty R, Braskich T, Emeott S and Tripunitara M. 2007. A proof of security of a mesh security architecture. Technical Report, IEEE press: 2007.

[7] Zorana B, Davis F, Jose M,M, Juan C V, pedro M, Alvaro A, Juan M. G. Elena. R. Javier B, Daniel V, iOctavio N.T.2011. Improving security in WMNs with reputation systems and self-organization Maps. Journal of network and Computer Applications (2011), 455-463.

[8] Sen J.2009. A survey on wireless sensor network security. International Journal of Communication Networks and Information Security, 59-82.

[9] O.E. Muogilim, K. K. Loo, R, Comley. 2011. Wireless mesh network security: A traffic engineering management approach, Jouranal of Network and Computer Applications, 478-491.

[10] A Gerkis, J. Purcell.2005. A Survey of Wireless Mesh Networking Security Technology and Threats, Technologies and challenges related to wireless mesh networks.

[11] I. F. Akyildiz, X, Wang, and W, Wang, “Wireless mesh networks: a survey”, Computer Networks, volume 47,no 4, pp. 445-487, March 2005.

[12] S. Mewada and Umnesh. K..S.2012. performance Analysis of Secure Wireless mesh Networks, Research Journal of Recent Science, 80-85.

[13] Http://connectonetworks.com/index.php/wmm

[14] Leutele Lucia Maria Grey.2013. Security Challenges in Wireless Mesh Networks- Literature Review.

[15] Ian F. Akyildiz, Xudong Wang. 2005. A survey on wireless mesh networks.

JETIR