THE SECURE TECHNIQUES FOR WIRELESS MESH NETWORKS: A REVIEW

[1]**Shubhpreet Rana**
Department of Computer Science and Engineering
Baddi University of Emerging Sciences and Technology

[2]**Aditi Kumar**
Department of Computer Science and Engineering
Baddi University of Emerging Sciences and Technology

Abstract: A wireless mesh network (WMN) is a communication network where mobile nodes are organized in a mesh topology. A WMN is one of the forms of wireless mobile ad-hoc networks (MANETs). A mesh network possesses a strong interconnection among devices or nodes. A small network coverage area is sometimes termed as a Mesh Cloud where each node is connected to more than one neighboring nodes, In this work we will study about the architecture, different routing protocols and significant qualities and threats of a wireless mesh network.

Keywords: Wireless mesh network, mesh topology, routing, routing protocols, Dos attack.

INTRODUCTION

A wireless mesh network is a popular network in use. In this era of mobile ad-hoc networks wireless mesh network is a part of it. In this network topology is comparatively more static so that routes can converge and thus data delivery can occur at faster rate.

Architecture:

Wireless Mesh Network sometimes depends on static nodes to act as a gateway so it is not truly all wireless ad-hoc networks. Wireless mesh networks basically consists two types of nodes:
(1)Mesh Routers
(2)Mesh Clients

Wireless Mesh Routers works as Access Points (AP) for wireless mobile nodes. Some of these routers act as the gateways to internet. These are connected through high speed wired links.[1] These gateways are not necessarily connected to the internet.

Wireless Clients are mostly laptops, cell-phones, and other devices.

To understand Wireless Mesh Network completely we first need to understand Mesh topology. In mesh topology devices are inter-connected with each other. In a well connected topology every node has a connection to every other node in the network either direct or indirect. If one node fails to respond then the network remains unharmed because other nodes can backup for that failed node.

Routing in WMNs:

In wireless mess networks routing is a challenging issue because of unpredictable movements in the wireless nodes. To overcome these and to enhance the routing techniques we can use two approaches:

In one approach we can improvise the path detection matrices. Second thing we can do is that we can modify the route algorithms by considering the new characteristics of WMNs. Here we choose the routing protocols depending upon the size of the network, density of the nodes, and the traffic patterns in a wireless mesh network. Therefore the larger is the network the lesser it is flooded.

Routing Protocols:

There are many routing protocols proposed since this day but there are few we will discuss here. DSR is dynamic source routing as the name itself suggests it is dynamic in nature. It does not require any periodic update of the route. As the source is ready to send the message, it will check for the valid route. If route exists, the source will use it, if not then source will send a request packet. In this protocol the matrices depends on the hop-count. But this protocol lacks in handling congestion from high traffic load. DSR is non scalable as network size increases, so as the delay. LQSR link quality source vector is an extension of DSR by adding some matrix to it.

AODV stands for ad-hoc on demand distance vector. This protocol sets up routes on demand and only the active ones are maintained. It uses route request and reply mechanism to discover the route. It also uses an Expected Transmission Time (ETT) matrix. AODV-MR(Multi-Radio) protocol works with assuming that every node shares minimal one common channel with its neighbors. So in AODV-MR traffic is distributed across multiple non overlapping channels as to reduce the degree of interference and contention.

Destination Sequenced Distance Vector Routing (DSDV) maintains a route table containing the shortest table to every destination Its disadvantage is that there is no mechanism to balance the node and as the network size increases its delivery ratio decreases.[3]

Wireless mesh network can be seen as a combination of wireless Local Area Network WLANs wireless metropolitan area networks WMANs and wireless sensor networks (WSN). WMN has certain limitations to have some fixed nodes gateway requirement and also faces difficulty in handling the user mobility. Bandwidth limitation is another issue .[4]

Significance Of wireless Mesh Networks:

1. Self Organizing and self configuring: WMNs are not design dependant and as it adjusts accordingly thus reducing the setup time and support cost. WMN are self configuring also which makes it upgrades the system execution and thus helps the system to change, grow and adjust as per expectations.
2. Enhanced Reliability: An important feature of mesh network is that it does not depend on any specific node. There is no centralization every node is interconnected and thus if one node fails there are always many alternatives to that.
3. Scalability: As in older remote systems when there is an increase in communication nodes the whole system execution gets affected on larger extent. But in WMNs the result is beneficial because increased no of nodes helps to reduce congestion and hence increase the throughput.[5]

Security Attacks on Wireless Mesh Network:

The architecture and structure of WMN is also prone to security attacks. Some of the common attacks are distributed denial of service (DDoS), signal jamming, traffic flooding attacks e.t.c. We will discuss about the Distributed denial of service attack in detail.

Denial of service (DoS) Attack

This attack is one of the most vulnerable attacks and become a major threat to current computer networks. To discuss all the attack techniques is not possible, so we discuss a few main techniques of DoS, those are:

TCP SYN Flooding:-

When client tries to establish a connection with the internet server it sends SYN message and wait for the SYN-ACK (acknowledgement). At this point the server is in half open state and the attacker can create many half-open connections by getting the source IP address. As the space in the process table is less and that will be filled by the too many half opened connections made by the attacker. Thus leaving the victim with no option, but deny its services.

ICMP Smurf Flooding:-

In this attack the attackers spoof the IP address of the victim and send ICMP echo request messages to large no of computers on internet. Thus all those computers starts replying with echo reply messages to the source IP address and hence make it impossible to work.

UDP Flooding:

Here the attackers send UDP datagrams IP packets to the random ports on the targeted host. When host tries to check the application related to the datagram, finds nothing and it will send a packet “destination unreachable”. As large no. of datagrams are received and answered system becomes slow and unreachable to other clients.

D (DOS) Attack

Distributed denial of service attack is the one in which one system acts as a master and find a no. of vulnerable computer systems which are prone to get affected or exploited by the master. These systems will acts as a bait and loaded with DDoS daemons and carry out the actual attack on larger no. of systems in the outside world.[6]

Security Measures in WMN

WMN is a migration of ad-hoc networks so till date it uses same security standards. But it possesses a different architectural and structural design, so WMN needs to have their security for the multi-hop routing operations. The different security measures in WMN are authentication, cryptography, WEP and WPA2, IP access-list filtering and control, IP virtual private networks traffic (VPN). e.t.c. The VPN-IPsec can lower the overhead and processing of the WMN using many techniques. The VPN-IPsec improved version can secure both the data traffic and the infrastructure of WMN [7]

LITERATURE REVIEW:

Er. Pushpender Sarao, Dr. Sohan Garg, Prof. (Dr.) YashPal Singh, (2013) presents[1] a paper in which wireless mesh technology is discussed over many aspects such as its concept, architecture, issues related, and challenges faced. WMNs have so many positive aspects that it is said as most likely used technology of today. This work here describes the most recent overview of technology, concept, and architecture for WMNs. Although WMNS have quiet large no. of advantages there are certain Issues and challenges in it such as: power management of mobile nodes, node mobility management, secure routing, its connectivity with the Internet and with other networks, its service levels, etc., at different layers of a network. In this work author focused on recent critical challenge on routing and the deployment issues.

Kartik Pandya(2013) here represents [2] different topologies taken in account to create a network including mesh topology. He discussed all of them with their qualities and disadvantages and came out with a conclusion that all of them are useful for specific requirements and hence can be used accordingly.

Shubat S. Ahmeda and Eman A. Essied (2013) [3]represents here the comparison between the two default matrices for AODV routing protocol those are expected transmission time matrix for AODV single radio and interference aware matrix for AODV multi-radio. Certain tests were applied on both the matrices for over 200 nodes using some simulation tools and came out with the conclusion that AODV-MR gives better results with interference aware matrix.

Sonia Waharte & Raouf Boutaba & Youssef Iraqi & Brent Ishibashi(2006) [5] presented this paper on the characteristics of wireless mesh networks those show their significance on routing .A set of criteria is designed to test all the existing routing protocols for ad-hoc network. Sensor network and wireless mesh network. All these tests serves as a base for deriving key design for the routing in wireless mesh network and guide for future work in this area.

Okechukwu E.Muogilim a,n, Kok-KeongLoo b, Richard Comley (2011) presented[7] this paper regarding the threats which are common to all wireless networks including wireless mesh network and discussed about their effects on various layers of the network. He also suggested techniques so as to reduce the effect of these attacks and counter them. He suggested an interconnection between wireless mesh network and VPN IP-sec so as to defend the network against these attacks.

Shenam Chugh, Dr. Kamal Dhanda(2012) [6] presented in this paper the attacks techniques of denial of service DoSattack. They discussed how these attacks actually work. To defend a system against these attacks efficiency and scalability are the key requirements. An approach is also suggested here that cooperation and communication with the researchers all over the world can help us to come out with better results against these attacks.

Author's name	Year	Description	Outcome
Er.Pushpender Sarao, Dr. Sohan Garg, and Prof. (Dr.) YashPal Singh,	2013	This paper gives an overview of the wireless mesh technology and architecture. WMN issues and challenges are deliberated briefly.	At the end of this paper comparison of all the protocols is done and the results are evaluated.
Kartik Pandya	2013	In this work different network structures or we say topologies are discussed and compared.	In the conclusion we found that all topologies have some merits and demerits thus it depends upon the need of the system that which topology is suitable for its proper functioning.
Shubat S. Ahmeda and Eman A. Essied	2013	In this work single radio and Multi-radio AODV routing protocols are compared on the basis of ETT and interference aware matrices respectively	AODV-MR routing protocol gives better Performance with *i*AWARE metric, on the perimeters end to end delay, packet loss and throughput.
Sonia Waharte & Raouf Boutaba & Youssef Iraqi & Brent Ishibashi	2006	In this work wireless mesh network's routing characteristics are identified and compared with the characteristics of routing protocols from other existing techniques i.e. ad-hoc net., sensor network e.t.c,	WMNs possesses various characteristics that helps it to be better than those other existing wired or wireless networks,
Naveen T.H and Vasanth G	2017	In this survey paper, important features of a Wireless Mesh Network are compared with some of the existing implementations in WMN	At the end of this survey by doing the comparison we found that there are many scopes available for the future solutions for variable loads.
Okechukwu E.Muogilim, Kok-KeongLoo RichardComley	2011	Various threats to wireless mesh networks are discussed over here and there counter parts are discussed also.	With this work we concluded that due to the architectural structure the security of WMN is weak but we can enhance it by using it with a combination to other security networks such as VPN IP-sec.
Shenam Chugh, Dr. Kamal Dhanda	2012	DoS attacks on wireless mesh networks are discussed over here and their characteristics.	It is concluded that these attacks are major threats and thus needed to be taken seriously and in future solutions must be found to resolve these attacks.

CONCLUSION

In this work we discussed about the architecture, techniques and topologies used to make a wireless mesh network. Routing protocols are discussed and compared. Qualities of a mesh network are also defined and their significance is discussed. The major security threats are defined over here and their solutions are suggested. It is also suggested that combination of a wireless mesh network with other security networks can help resolving the issues and threats and improve the efficiency of both the networks. For future scope we can use this information to enhance VPN with a combination to the WMN and its Routing protocols to enhance security of both the networks.

REFERENCES

[1] Er.Pushpender Sarao , Asstt. Professor in SITM, Rewari, India Dr. Sohan Garg, Professor, C.C.S. University, Meerut, India
Prof. (Dr.) YashPal Singh, Professor, S.(P.G.)I,T.M., Rewari, India, “Wireless Mesh Networks: WMN Architecture, Issues and Challenges”2013, 2319-4413

[2] Kartik Pandya Lecturer in Sikkim Manipal University (S.M.U) ,” Network Structure or Topology”India 2013, ISSN: 2321-7782

[3] Shubat S. Ahmeda Ph. D. from theDepartment of Electrical and Electronics Engineering, University of Nottingham and Eman A. Essied BSc in Computer Engineering from University of Tripoli, Libya “Routing Protocols for Wireless Mesh Networks” 2013 vol.1 no1.

[4] Sonia Waharte & Raouf Boutaba & Youssef Iraqi & Brent Ishibashi “Wireless mesh network security: A traffic engineering management approach”, 2006, 478-491.

[5] Naveen T.H Research Scholar Visvesvaraya Technological University Belagavi, Karnataka, India Vasanth G Prof & Head Dept. of Computer Science & Engineering Government Engineering College, Krishnarajpet,Mandya District, Karnataka, India ,” Qualitative Study of Existing Research Techniques on Wireless Mesh Network” Vol. 8, No. 3, 2017

[6] Shenam Chugh, Dr. Kamal Dhanda Department of CSE, BRCM Bahal, Bhiwani, Haryana, India “Denial of Service Attacks”2015, V5. I8, ISSN: 2277 128X

[7] O.E.Muogilim, K.-K. Loo, and R. Comley, "Wireless mesh network security: A traffic engineering management approach," Journal of Network and Computer Applications, vol. 34, pp.478-491, 3// 2011.