International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Security Technique and Congestion Avoidance in Mesh Network

Mankiran Kaur
Assistant Professor, CSE, Chandigarh Group of College, Landran, Mohali

Jagjit Kaur
Assistant Professor, CSE, Chandigarh Group of College, Landran, Mohali

ABSTRACT

Security in wireless network is one of the prime concern in today's Information Age, where information is an asset not only to an organisation but also to an individual. Security to a great extent is able to protect the network from various unauthorized attacks. On the other side implementation of security mechanisms also causes an overhead in terms of increased load in the network. Further the increased load in the network paves path to congestion which degrades the performance of the wireless network. In this paper we try to highlight various challenges pertaining to security in mesh networks and the ways of reducing security threats. We propose an improved version of AODV which has a congestion avoidance mechanism. We also use a security technique called PGP for enhanced security of Mesh network.

Keywords: *AODV, PGP, SBPGP*

1. INTRODUCTION

Wireless mesh networks (WMNs) consist of wireless nodes and wireless access points. WMN's nodes are composed of mesh routers and mesh clients. Each node works as a host and router as well. Nodes in mesh network consist of in built routing functionality which forward packets to other nodes that are within their range .WMN is self-organized network in which nodes automatically establish connectivity among each other. Nodes in the mesh network co-operate with each other in the network to forward packets. The other protocols for example MAC layer and network layer protocols usually assume that the nodes that are taking part in communication are honest and well-behaved with no malicious or intention to make any harm to the network. Usually in network some nodes may behave selfishly and consists of unauthorized users. The nodes in the network assumes that the node is trusted so and they start communicating with them .In this way alicious nodes enter the network and can harm the

2. SECURITY IN MESH NETWORK

WMN is exposed to various kinds of threats and risks messages can be changed, there can be delay in transmission, fake messages can be inserted. Resources of the network can be accessed without authorized access and can lead to complete denial of service (DOS) .So Security in Mesh Network is very important The Authentication and Key Management in Wireless Mesh Networks is a crucial aspect of any security solution.

2.1. Security Protocols

Since various protocols available to tackle wireless network security, but there is a chance of intrusion in the network. Possible ways for securing network could be to secure all wireless LAN devices Network can be secured by implementing strong security in the network. There must be some mechanism in each node so that they can identify malicious nodes that have the intention to harm the network. Some of the techniques are explained below:

2.1.1 Mac Address Filtering

In the network there are various access points .These access points contains some inbuilt technique that allows the administrator to only give access to the node which have a valid MAC ID's. This method is good for identification of the node but it has a drawback that id can be hacked. There are various cracking methods available like SMAC.

2.1.2 Static IP Addressing

The method of static IP addresses for the network devices and end clients manually makes it tough for a attacker to log on in the network. But this is not a robust mode of securing the network. There are lot of tools available to spoof the IP addresses. Using these spoofed IP intruder can easily harm the network security.

2.1.3 WEPI

WEP (Wired Equivalent Privacy)[18][19] is a encryption protocol which is based on the RC4 encryption algorithm, with a secret key of 104 bits or it can be 40 bits combined with a 24-bit Initialization Vector (IV) to encrypt the plaintext message .Various users have observed many drawbacks in WEP the use of RC4 is accepted as a strong cryptographic cipher. However, Attackers can attack not only on whole cryptographic algorithm, they can also attack any weak point in the cryptographic system. But technique of violating WEP has came into existence.

3. WMN SPECIFIC SECURITY CHALLENGES

Due to the shared nature of wireless transmission medium, the absence of globally central authority, and the lack of security of mesh routers lead to main challenges for securing WMNs. Firstly the Correct routing messages are difficult to achieve in multihop routing scenario, the most harmful kind of malicious information is due to the fabricated routing messages[23].Secondly, an authentication mechanism is implemented with the help of Public Key Infrastructure (PKI), which requires a globally trusted authority to issue certificates. Having a globally trusted authority is not possible all the time in Wireless Mesh network Thirdly, the mesh devices are usually placed openly without any protection so they are not physically protected So it becomes very much easy for the intruder to have full control over the device, thereafter launching attack from the router and the data sent by router will be considered as authenticated by other nodes. And if the device is equipped with some cryptographic technique it is easily broken by the attacker. Therefore some authentication is required. Pretty good privacy is a cryptographic technique which can apply in wireless networks. PGP is explained as follow:

3.1 PGP Based Security

Pretty good Privacy (PGP) is a security model that is used for encryption and decryption of data which sends from source to destination. It responsible for securely transmit data from source to destination. It activates the central authority (CA) for providing certificate to each node when it is used in wireless ad-hoc network. It provides security to ad-hoc network and improves the performance of network. They use public key infrastructure (PKI) to resist the collisions intentionally caused by malicious nodes. It using certificates, digital signature and key issuing can authenticate message, identify valid nodes or malicious nodes. It is symmetric and asymmetric cryptographic, web of trust model. This model fulfils various security requirements such as authentication, privacy, confidentiality and Non-repudiation of Mesh network.. It protects the message (or its contents) from being altered or destroyed. PGP algorithm (128 bits) is implemented for security which is faster as well as secure than previously implemented algorithms. It entails the state level registration authority acting as certificate authority (CA).

PGP security provides the same session key for encryption and decryption between source and destination node. In this each node request for the session key from central Authority to communicate with neighbouring node. Source sends the session key request for neighbouring node then CA checks the authorization of node. CA provides the session key for communication between Source and neighbouring node. When source sends the message to neighbouring node then it encrypt the message with private key of source node and after that whole message are encrypted with that session key. So this process is continued until the destination node is reached.

3.1.1 How PGP works

PGP combines the aspects of conventional authentication and public key cryptography .In PGP user encrypts plaintext with PGP .The PGP compresses the plaintext .Compressing data saves transmission time of modem and disk space and enhances the cryptographic security .after compressing the plaintext PGP creates a session key, which is one time secret key .This one time secret key works very securely with encryption algorithm to encrypt plain text and results in ciphertext. After encrypting data the one time secret key is encrypted

with receiver's public key. Then ciphertext and public key encrypted secret key is transmitted to the receiver. Decryption is reverse of this Process.

3.1.1 Various Attributes of PGP Type Certificate

1) Certificate serial number

2) PGP Version

3) Certificate holder Public key

4) Holder information

5) Digital sign [26] of certificate owner Key.

6) Verifying Signature

3.3. Applying Security Technique

It has been observed that applying security technique in a network overload the network with lot of route request and buffer gets full due to certificate issuance and revocation procedure in network . Suppose one node is performing certificate revocation process and at the same time it gets route request from the other node this can lead to buffer overflow and can cause congestion in the network.

4. Different Routing Protocols in Mesh Network

Ad hoc routing protocols are usually

1) Reactive
2) Proactive
3) Hybrid

A. Reactive Protocols

Reactive protocols are also known as on demand driven routing protocols. They are called reactive protocols because they Start route discovery by not by themselves, route discover is done on demand when requested by other nodes, when a source node send the request to create a route. Route setup is done when demanded.

B. Proactive Protocols:

In Proactive protocols, every node in the network maintains routing table of itself and routing table of other nodes in the network .Each node maintains most recent routing information by sending control messages after small interval among the nodes . The proactive routing protocols uses link state routing information which frequently links the information about neighbors. Some of the existing routing proactive protocols are DSDV and OLSR.

C. Hybrid Routing Protocol:

Hybrid routing protocol is a combination of proactive and reactive routing protocols. In the beginning routing is done with proactively prospected routes or predefined routes and when any node wants to make connection route establishment is done through reactive flooding Some of the examples of hybrid protocols are TORA protocol and ZRP protocol.

4.1 AODV protocol

- Ad-Hoc on Demand Distance Vector Protocol (AODV):

AODV is a reactive routing protocol, when a node in the network wants to communicate with other node in the network it sends the route request to other .Each node has the topology information which is provided by AODV. Control messages are used in the network to find a route to the destination in the network. But sometimes network is flooded with lots of route request and it leads to congestion in network.

Congestion avoidance can be done which is not done in AODV .It can be performed by creating a Cycle on a node where the congestion probability is high . Each node contains the routing table including information about its own I.P. address, I.P. address of nearer neighbor nodes, distance between the nodes, & queue length of each node.

4.1.1. Congestion Avoidance

Congestion is created when the capacity of the link or node exceeds beyond its limit. when the rate of sending increased and receiver is unable to receives the data as nodes threshold limit has reached, than buffer starts overflowing which results in long queuing delays and packet loss to the large extent. So there is need to monitor incoming and outgoing traffic across the link. Downlink nodes are equal than the traffic is balanced as the node has many options to route traffic through downlink nodes. But if uplink nodes are more and there are less number of downlink nodes, then congestion is created .Because than the node have less options available nodes to route traffic To overcome this problem .We have taken the ratio of downlink and uplink nodes.

• We have proposed the term Ratio of downlink and uplink node (RDU) as the ratio of downlink and

uplink nodes for a particular node. Uplink nodes are depicting incoming traffic and downlink node depicts outgoing traffic.

RDU=Total of downlink nodes/Total of uplink nodes

The individual RDU values at each node are used to make forwarding decisions. When a node wants to transmit packet it calculates its RDU before transmitting Data.

1) If RDU is greater than one, it means that the node has a greater number of downlink nodes in comparison with uplink nodes. If so, it can implement any Fair Queuing (FQ) mechanism and forward packet to appropriate downlink node normal routing process is carried out.

2) If RDU is less than one, it depicts that there are more uplink nodes as compared to downlink nodes. So rate reduction is required to prevent congestion.

8. CONCLUSION

In this paper we have discussed, the concept of trusted model and authentication architecture in Wireless Mesh Networks. The wireless Mesh network is more susceptible to various kinds of attacks if proper security mechanisms are not implemented. On the other side adding security feature in the protocol has a decremental affect on the network performance due to increased load in the network. Keeping this in view we have proposed that congestion avoidance algorithm should be applied on nodes which will increase the overall performance of the network.

9. FUTURE SCOPE

In this paper we have discussed various routing protocols used in mesh network and various security techniques. We can apply different security technique in the Mesh Network to enhance security in the network.. Dynamic path selection routing mechanism can be applied to decrease end to end delay and enhance overall network performance.

REFERENCES

1) Ding Xuyang, Luo Huiqiong. "Trust Evaluation Based Reliable Routing in Wireless Mesh Network" Proc. Of IEEE International Conference of Wireless Communication, Networking & Mobile Computing (WICOM 2007),21-25 September 2007, Shanghai, China.

2) Nathan Lewis, Noria Foukia, and Donovan G. Govan. "Using Trust for Key Distribution and Route Selection in "Wireless Sensor Network" Proc. Of IEEE/IFIP Network Operations and Management Symposium(NOMS 2008), April 2008, Salvador, Brazil.

3) QIU Xiu-feng, LIU Jian-wei, Abdur Rashid Sangi. "MTSR: Wormhole Attack Resistant Secure Routing for Ad Hoc Network" Proc. of IEEE Youth Conference on Information Computing and Telecommunications (YC-ICT), pp 419-422, 28-30 November 2010.

4) Shi-Hong Chou, Chi-Chun Lo, Chun-Ch ieh Huang."Mitigating Routing Misbehavior in Dynamic Source Routing Protocol Using Trust-Based Reputation Mechanism for Wireless Ad-Hoc Networks" Proc. of 8th Annual IEEE Consumer Communications and Networking Conference - Security and Content Protection

5) Shantanu Konwar, Amrita Bose Paul, Sukumar Nandi, Santosh Biswas. "MCDM based Trust Model for Secure Routing in Wireless Mesh Networks" Proc. of IEEE World Congress on Information and Communication Technologies (WICT), pp 910-915, 11-14 December 2011, Mu mbai, India.

6) U.Venkanna, R.Leela Velusami. "Black Hole Attack and their counter measure based on trust management in MANET: A Survey" In Proc. of International Conference on Advances in Recent Technologies in Communication and Computing (IET 2011)" ,

7) Naveen Kumar Gupta Kavita Pandey. "Trust Based Ad-hoc On Demand Routing Protocol for MANET" Proc. Of IEEE Conference 2013.

8) Meenakshi Mehla, Himani Mann. "Sbpgp Security Model Using Iodmrp" International Journal Of Computational Engineering Research, Vol. 2,Issue No.3, pp-823-828, May-June 2011.

9) Jashanvir Kaur and Er. Sukhwinder Singh Sran. "SBPGP Security based Model in Large Scale Manets" International Journal of Wireless Networks and Communications, Volume 4, Number 1 (2012).

10) Ranjeet Singh Harwant Singh Arri. "Analysis of QOS Parameters of AAMRP and IODMRP using SBPGP Security Model" International Journal of Computer Applications, Volume 69– No.15, May 2013.

11) Nidh Mittal, Janish. "Performance Evaluation of AODV and DSDV under Seniority, Based Pretty Good Privacy Model (SBPGP)" International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.

12) Tanupreet Singh, Shivani Dua, Vikrant Das, "Energy-efficient routing protocols in Mobile ad-hoc Networks", International journal of Advanced research in Computer Science and Software Engineering, Vol. 2, Issue 1, January 2012.

13) P. Kuppusamy, K. Thirunavukkarsu and B. Kalavathi, "A study and Comparison of OLSR, AODVand T ORA Routing Protocols in Ad hocNetworks", Proceedings of 3rd IEEE Conference on ElectronicsComputer Technology (ICECT 2011), 8-10 April 2011.

14) F. Maan, Y. Abbas and N. Mazhar, "Vulnerability Assessment of AODV and SAODV Routing Protocols against Network Routing

Attacks and Performance Comparison", in IEEE Wireless Advanced (2011).

15) Yih-Chun Hu, Adrian Perrig, and Dav id B. Johnson, Member, "Wormhole Attacks in Wireless Networks" IEEE Journal on selected areas in Communications,. Routing in Wireless Mesh Networks" Proc. of IEEE World Congress on Information and Communication Technologies (WICT), pp 910-915, 11-14 December 2011, Mumbai, India.

16) Majid Khabbazian, Hugues Mercier and Vijay K.

17) Stewart S. Miller "Wi-Fi Security" The McGraw-Hill Companies, 2003.

18) Sultan Weatherspoon, "Overview of IEEE 802.11b Security" Network Communications Group, Intel Corporation.

19) F.Maa Y.Abbas and N. Mazhar, "Vulnerability Assessment of AODV and SAODV Routing Protocols against Network Routing Attacks and Performance

20) Yih-Chun Hu, Adrian Perrig, and Dav id B. Johnson, Member, Wormhole Attacks in Wireless Networks, IEEE Journal on selected areas in Communications.

21) Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure, Proc. of IEEE Global Telecommunications Conference (GLOBECOM '06), PP 1-6, San Francisco, CA, USA, 27 November - 1 December 2006

22) Mohammad Z. Ahmad. "Congestion Avoidance and Fairness in Wireless Sensor Networks", IEEE GLOBECOM 2008 – 2008 IEEE Global Telecommunications Conference, 11/2008

23) Chou, Shi-Hong, Chi-Chun Lo, and Chun- Chieh Huang. "Mitigating routing misbehaviour in Dynamic Source Routing protocol using trust-based reputation mechanism for wireless ad-hoc networks", 2011 IEEE Consumer Communications and Networking Conference (CCNC), 2011