ISSN:0975-9646

A Review of Packet Filtering Problem in MANET

Purnima[#1], Rimple[*2]

[1]*Innocent Heart Group of Institution,*
Punjab, India
[2]*Lovely Professional University,*
Punjab, India

Abstract -The wireless Ad hoc network is the self configuring type of network .In self configuring type of networks mobile nodes can leave or join the network when they want .In such type of networks many inside and outside attacks are possible. Inside and outside attacks are broadly classified as active and passive attacks. Attackers can perform many active and passive attacks; these attacks are channel jamming attack, black hole attack, Man-in- middle attack. Packet filtering technique is the efficient technique to prevent active and passive attacks. In this paper, we review various problems for implementing the packet filtering in MANET and propose new technique for Packet filtering.

Keywords
Packet filtering, Attacks, black hole, Man-in-Middle, MANET

INTRODUCTION

Ad hoc network is a decentralized type of wireless network. In ad hoc network there is no pre-existing infrastructure, such as routers in wired networks or access points in wireless networks. In ad hoc network each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. Basically it's a network which is used in emergency causes. Here is No fixed infrastructure in ad hoc network like base stations as mobile switching. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

- **Passive attacks:** A passive attack does not disrupt the normal operation of the network; the attacker spoof the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated.
- **Active attacks:** An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Impersonation, modification, fabrication, and replay of packets.

The use of laptops, PDAs and mobile devices has changed the business sector to improve the market of wireless networks in an ad hoc mode. MANETs have gained much importance because of the features such as they are decentralized, self organizing, adaptive and dynamic in nature. The delay, power consumption and traffic are main concerns in ad hoc networks due to its non confined nature. The MANET station acts like a router to route the information from one node to the other node as there is no access point available in ad hoc networks. Mobile ad hoc networks are dynamic in nature as the nodes are dynamically allocated without the central administration and the nodes will behave as the hosts for the file transfer protocol, email, HTTP and other applications to transmit and receive the information [2].MANETs have the limited energy budget [7] for communication among mobile nodes, thus usage of the energy resources of a small set of nodes at the cost of others can have an adverse impact on the node lifetime as well as network lifetime. The Packet filtering is difficult to implement because no central controller is present in MANET. The firewall is generally implemented on the central controller. Where all the network traffic cross and the malicious packets can be filtered at the central controller before forwarding to the legitimate users.

1. LITERATURE REVIEW(RELATED WORK)

K.Arulanandam and B.Parthasarathy (2009) [5] gave an approach to minimize power consumption in idle mode of mobile nodes. They gave an idea to change mode of the mobile nodes from Idle to Sleep, because when nodes were neither transmitting nor receiving data packets but in Idle mode consume power as been consumed in receiving mode. They have taken two ad hoc on-demands routing protocols and performed this approach and illustrated that power consumed by these protocols, with this mechanism is less than power consumed by any other mechanism. It saved power up to 60%. Canan Aydogdu and Ezhan Karasan (2010)[6] proposed an analytical model for the IEEE 802.11 DCF in multi-hop wireless networks that considered hidden terminals and accurately worked for a large range of traffic load that are used to analyze the energy consumption of various relaying strategies. The results shown that energy consumption not only depends upon processing power but also on traffic load that is the number of nodes presented in network.Seung Hwan Lee and his colleagues proposed an energy efficient power Control mechanism for base station in mobile communication systems and an efficient sector power control based on distance between base station and mobile node. They proposed a sleep mode energy control mechanism. In sleep mode energy saving protocol, each sector monitors the number of users in sector cell. They proposed, if number of mobile node falls down a given threshold in sector cell, base station shuts down the power. They also proposed algorithms and demonstrated the tradeoff between energy saving and cell coverage in order to enhance efficient use of base station transmission power.Xavior pallot and Leonard E.Miller (1998) [1] proposed a design to evaluate the effectiveness of a MANET in delivering priority message service using a standard routing algorithm such as DSR but altering the protocols used at Medium access (MAC) and Physical (PHY) layers according to the IEEE 802.11 specification. in Yu (2004) [6] proposed mechanisms to make routing protocols aware of the packet lost data packets and ACKs and help reduce TCP timeouts for mobility-induced losses. He presented two mechanisms: Early packet loss notification (EPLN) and Best effort ACK delivery (BEAD).Shweta Jain and Samir R.Das (2010) [3] proposed an anycast mechanism at link layer that forwards packets to the best suitable next hop link to enable efficient packet forwarding on a multihop route. They proposed a mechanism that depends on the availability of multiple next hops, which could be computed by a multipath routing protocol. The anycast protocol provides signifcatnly better packet delivery relative to 802.11 in variety of ad-hoc networks models, both regular and random, stationary and mobile.Kaixin Yu, MArioa Gerla, Sang Bae (2008) [4] shown the effectiveness of RTS/CTS in wireless ad-hoc networks. First, they analyzed the interference range for open space environment. Second, verify the data packet corruptions due to large interference range. Third, a simple MAC layer scheme proposed to combat the large interference range. They have done only trivial modification to 802.11 standard.Seyed-Amin Hosseini-Seno, Tat-Chee Wan, Rahmat Budiarto (2011) [9] employed sleep mechanism for all member nodes except gateway nodes that are in idle mode. They used energy efficient CBRP(cluster based routing protocol) and shown that CBRP is more powerful and scalable routing protocol for ad hoc and its comparison to AODV which is a standard protocol, the overhead of CBRP is less and throughput of it is more than of AODV. Another they considered one manner for saving energy in cluster based ad hoc network is all of member node except gateways node can goes to sleep mode when they are in idle mode and with this method only CHs and gateway nodes are active for any communication in other words the backbone of the network every time is active to any communication**.**

2. PROBLEM FORMULATION

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. In ad hoc networks, the mobile nodes on the network dynamically establish the routing process by themselves. There is the possibility of more security threats in case of mobile and ad hoc networks (MANET) as compare to centralized wireless networks. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust. There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. The main problem in MANET is its decentralized feature. In decentralized feature network it very difficult to implement packet filtering. The attacks in the network can be prevented through packet filtering. Firewalls are generally used for packet filtering. In the centralized type of networks on the central controller, firewall is implemented. The network traffic has to pass through the central controller where it get filtered and then pass to the end users. In this paper, we formulate the problem to implement firewall in mobile ad hoc networks.

3. PROPOSED TECHNIQUE

The proposed mythology is based on clustering. The mobile nodes are work together and form a cluster. The cluster heads are selected by using election algorithm. In election algorithm every node has to present its resources to their corresponding nodes. The node which is having higher resources is selected as cluster head. The mobile nodes are identified on the basis of their IP address. Every cluster head in the network maintains a table in which the IP address of every node is stored. The cluster head is responsible for data routing. When cluster head receives data from the corresponding cluster head it will check the data. The coming data if belongs to the malicious nodes, packets will be filtered.

4. CONCLUSION

In the paper, we conclude that packet filtering is done through the use of firewalls. In centralized type of networks packet filtering will be easily implemented. The mobile ad hoc network is the self configuring network in such type of network it is difficult to implement firewall due to the unique feature of MANET. In this paper, we purpose new technique to implement firewall in MANET. New proposed technique is based on the clustering.

REFERENCES

[1]D.Sunitha,M.Chandrasekhar,"Measurement and Modeling of Mobile Ad-hoc Networks: It's Performance analysis using NS2", (IJAEST) International Journal of Advanced Engineering Sciences and Technologies Vol No. 9, Issue No. 2, 259 – 267, 2011.

[2] Neeraj Tantubay,Dinesh Ratan Gautam and Mukesh kumar dhariwal " A Review of Power Conservation in Mobile ad hoc network(MANET)" , IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[3] K. Arulanandam and B. Parthasarathy," A New Energy Level Efficiency Issues In MANET", IJRIC, E-ISSN: 2076-3336, pp.104-109, 2009.

[4] Canan Aydogdu and Ezhan Karasan, "An Analysis of IEEE 802.11 DCF and Its Application to Energy-Efficient Relaying in Multi-Hop Wireless Networks", IEEE Trans. on mobile computing, 2010.

[5] Xavior pallot and Leonard E.Miller," Implementing message priority policies over an 802.11 based mobile ad-hoc networks", 1998

[6] Xin Yu," Improving TCP performance over mobile ad-hoc networks by exploiting cross- layer information awareness", Mobicom'04, Sept, 2004.

[7] Shweta Jain and Samir R.Das,"Exploitng Path diversity in the Link Layer in Wireless Ad-hoc networks".

[8] Kaixin Yu, MArioa Gerla, Sang Bae, " How effective is the 802.11 RTS/CTS handshake in wireless ad-hoc networks", Project under graduate student fellowship.

[9] Seyed-Amin Hosseini-Seno, Tat-Chee Wan, Rahmat Budiarto, "Energy Efficient Cluster Based Routing Protocol for MANETs", IPCSIT vol.2 (2011)