International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 6 3672 – 3675

An Approach to Develop Security Aspect of MANET using NS2 Field

Sachin[1]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
sachind12@outlook.com

Shabnam Sangwan[2]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
shabnam022@gmail.com

Sonu Rani[3]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
dahiya.sonu@gmail.com

Sanjay Kumar[4]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
sanjay.kanti@gmail.com

Abstract: A Mobile network is a open area network in which any user can enter to the system and increases the network traffic. Large amount of useless traffic over the network results the congestion on the network nodes. As the data is transferred over these nodes, it increases the network delay and the data loss over the network. To identify the safe path over the network, we have defined an association mining based adaptive approach under different parameters.
A Mobile network always undergoes from different kind of external and internal attacks. One of such internal attack is DOS attack (Denial-of-Service). A DOS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the network. In this type of attack a particular user flooded the bandwidth with useless traffic and disturbs flow of data to other users. So a reliable communication path over the network is required with minimum delay & loss. Data mining approach is used to present the solution for this problem with effective throughput and minimum loss over the network.
Keywords: *Association Mining, Effective Throughput, Congestion, Parametric*

*****

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network [1].
Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Denial of Service (DoS), are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources [1].

II. MANET

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes [1, 2].
The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and

transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network [3].

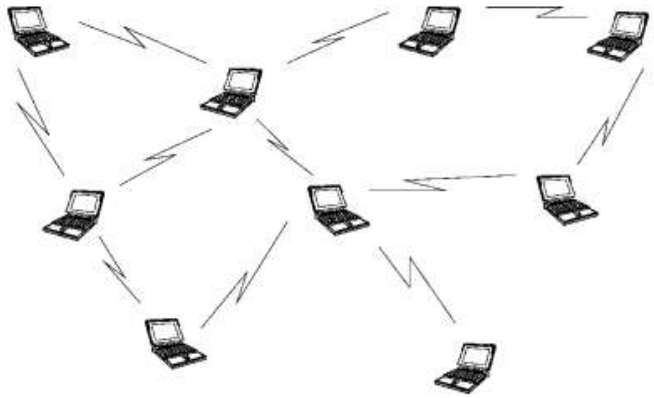

Fig 1.1: Mobile Ad-hoc Network (Manet) [8]

A. TYPES OF MANET [3]

Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment. VANET is a special class of Mobile Adhoc Networks (MANET), in which the nodes are the vehicles which communicate with other vehicles or with the base station which acts as a roadside infrastructure for using security and services application

Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc

Internet Based Mobile Ad-hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad-hoc routing algorithms don't apply directly.

B. Applications of MANET

Defence
- Military communication and operations
- Automated battlefields

Emergency services
- Search and rescue operations
- Disaster recovery
- Replacement of fixed infrastructure in case of environment
- Policing and fire fighting
- Supporting doctors and nurses in hospitals
- Home/office wireless networking

Conferences, meeting rooms
- Personal area networks (PAN), Personal networks (PN)
- Networks at construction sites

Education
- Universities and campus settings
- Virtual classrooms
- Ad hoc communications during meetings or lectures

Entertainment
- Multi-user games
- Wireless P2P networking

C. Characterstics of MANETS

MANETs have several salient characteristics [4]:

- **Dynamic topologies:**

Nodes are free to move arbitrarily; thus, the network topology--which is typically multi-hop may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

- **Bandwidth-constrained, variable capacity links**

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate.

- **Energy-constrained operation**

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

- **Limited physical security**

Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

III. CLASSIFICATION OF ATTACKS

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behaviour of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network [5].

- **External and Internal Attack**

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks [5].

- **Active and Passive Attack**

When the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network .Active attacks can an internal or an external attack. The active attacks are meant to destroy the

performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network [5].

IV. PROPOSED SOLUTION

In network, security is the main concern. In this work we will work with the DDOS attack. We will define the DDOS attack for MANET and define AODV protocol which is used to detect the DDOS attack. Distributed DDOS (DDOS) attacks are a relatively new development. DDOS attacks are similar to DDOS attacks but there is a difference between them and that is DDOS attacks involve breaking in to hundreds or thousands of machines, so for this reason, this attack called Distributed. Very often, systems that use for attack is a part of the networks and users of these systems don't know about that, their systems used for attack to another systems. This kind of attack, consume more bandwidth and uses more sources in network. One of the most important attacks of DDOS attacks category is DDOS attack. This attack effects on AODV protocol in WLAN. In this case, the attacker introduces itself as a real destination and uses all of the generated traffic for it. In addition, attacker produces some packets and sends them to the source and in this case consumes bandwidth and create bottleneck in network. In other words, such attacker doesn't allow that all of packets arrive at real destination On of these attacks is DDOS attacks that have an important and dangerous effect on Mobile Ad-Hoc Network and cause problems in these networks. In this work, we study the effect of one of the important attacks that called DDOS in WLAN on most vulnerability protocol that named AODV. The product of this study is detection of DDOS attack by using AODV (adhoc on demand distance vector) protocols [6].

A DDOS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets.This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. The distributed format adds the "many to one" dimension that makes these attacks more difficult to prevent. A distributed DDOS attack is composed of four elements, as shown in Figure 1.2

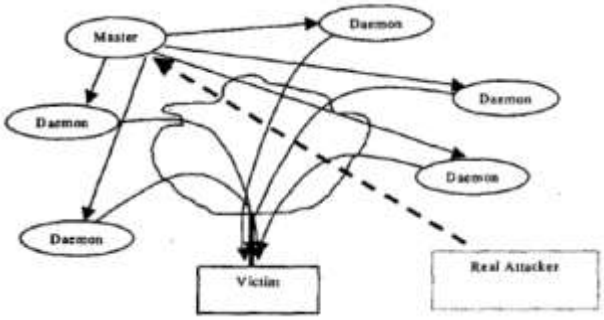

Figure 1.2 Four components of DDOS attack [7]

V. CONCLUSION

The proposed work is about the prevention of DOS attack. The proposed system is based on Association Mining based parametric analysis while performing the next node selection. The Association Mining parameters taken here are the loss rate, transmission rate and the network delay. The Association Mining on these all parameters is performed to identify the critical node as well as the safe node. On each node, the Association rule is implemented to identify the safe path. The process is repeated on each node till the destination is not achieved. The system is providing better throughput and less packet loss over the network. The system is implemented in a wireless network with AODV protocol. In this system a neighbor node analysis is performed under different parameters to provide the network security in case of DOS attack. Here we have proposed a new algorithm for the above said task. The implementation is performed in ns2 and analysis is presented using graph.

VI. FUTURE SCOPE

The proposed system can be enhanced in future by other researchers in the following ways

- We have performed the work only with DOS attack, the work can be enhanced by implementing some other attack such as worm hole etc.
- Further can be enhance a clustered approach in a wireless network. The work can be implemented on some specific network such as PAN, WiMax etc.
- Improve the Robustness of the Proposed Scheme
- Proposed scheme is able to defend against the active attacks, however not included the passive attack. So it would be interesting to extend the approach to the other security attacks. Then the feasibility of making the improved scheme for the WSN could be another direction for the future research.

Acknowledgment

I would like to thanks my guide Ms. Shabnam Sangwan, who suggested me to work and research. Her recommendations, innovative ideas and constructive criticism contributed to make the success of this report. Her numerous suggestions, comments, and advice have made this entire paper possible.

References

[1] L. Buttyan and J. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks,"

 ISSN: 2321-8169
3672 – 3675

ACM/Kluwer MobileNetworks and Applications (MANET) 8 (2003).

[2] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V.Vijayaraghavan, "Participation incentives for ad hocnetworks," http://www.stanford.edu/~yl31/adhoc (2001).

[3] J. G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Net

[4] M.S. Corson, J.P. Maker and J.H. Cernicione, Internet- based Mobile Ad hoc Networking, IEEE Internet Computing, pages 63- 70, July- August 1999.

[5] Y. Haung and W. Lee, A Cooperative Intrusion Detection system for Ad hoc Networks, in Proceedings of the 1st ACM Workshop on security of Ad hoc and sensor Networks, Fairfax, Virgining 2003.

[6] Y. Hu, A. Perrig, and D. B. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols". Proceedings of the ACM Workshop on Wireless Security 2003, Pages 30-40, September 2003

[7] Monika Khatri,Sona Malhotra, "Behavioural Study Of Vanet Protocols", IJRIM Volume 2, Issue 2 (February 2012) (ISSN 2231-4334)

[8] CHRISTINE E. JONES, "A Survey of Energy Efficient Network Protocols for Wireless Networks", Kluwer Academic Publishers. Manufactured in The Netherlands, 2001