Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.883 – 887

RESEARCH ARTICLE

An Analysis of Various Attacks in MANET

[1]M.Udhayamoorthi, [2]C.Senthilkumar, [3]Dr.S.Karthik, [4]Dr.T.Kalaikumaran
[1, 2]Assistant Professor/IT, [3]Professor & Dean/CSE, [4]Professor & Head/CSE
SNS College of Technology (Autonomous)
Coimbatore, TamilNadu, India
[1] udaya.manasu@gmail.com, [2] senthil.personal2010@gmail.com

Abstract*— An Ad-hoc network is a self-organized network, without a central coordinator, and which frequently changes its topology. According to the perspective of our paper, we try to connect the current status of computers era to adhoc networking. As adhoc networks has been unleashing several updated technologies, it is the most growing area in the field of networks in information and communication Engineering has ever seen .we start with area introduction, deeply reviewed about the various attacks especially in various layers of networks and concluded with the future trends just to show our area has not stopped with any period mark.

***Keywords*— MANET, DOS, MAC, CTS, RTS**

I. INTRODUCTION

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 they, i.e., routing functionality will be incorporated into mobile nodes. 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 critical environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. The 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.

II. APPLICATIONS

1) Military battlefield: Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

2) Collaborative work: For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

3) Local level: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

4) Personal area network and Bluetooth: A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the intercommunication between various mobile devices such as a laptop, and a mobile phone.

5) Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

III. BROADCASTING APPROACHES IN MANET

In MANET, a number of broadcasting approaches on the basis of cardinality of destination set:
1. Unicasting: Sending a message from a source to a single destination.
2. Multicasting: Sending a message from a source to a set of destinations.
3. Broadcasting: Flooding of messages from a source to all other nodes in the specified network.
4. Geocasting: Sending a message from a source to all nodes inside a geographical region.

IV. ATTACK CLASSIFICATION IN MANET

The attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. The various attacks on individual layer are as under:

- ✓**Application Layer:** Malicious code, Repudiation
- ✓**Transport Layer:** Session hijacking, Flooding
- ✓**Network Layer:** Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- ✓**Data Link/MAC Layer:** Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- ✓**Physical Layer:** Interference, Traffic Jamming, Eavesdropping

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of the network connection. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' accesses to a service provider. They have numerous forms and they are hard to prevent. For instance, an attacker may send an excessive amount of requests to a server that has to test their legitimacy. This test requires an amount of CPU and memory capacity. Due to the excessive number of requests, the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired networks, DoS attacks in MANETs may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider. They have numerous forms and they are hard to prevent. For instance, an attacker may send an excessive amount of requests to a server that has to test their legitimacy. This test requires an amount of CPU and memory capacity. Due to the excessive number of requests, the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired networks, DoS attacks in MANETs may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks.

Physical Layer

DoS attack can be launched against physical layer by using radio jamming device or by source of strong noise to interfere the physical channels and may compromise the service availability. For jamming attack in WMN, the attacker can launch the attack from anywhere. Due to the vast coverage area and dense deployment of wireless mesh routers in WMN, it is **more** vulnerable to physical layer DoS attacks. Different types of jamming attacks are:

1) Trivial Jamming Attack: In which an attacker constantly transmits noise.
2) Periodic Jamming Attack: In which an attacker transmits a short signal periodically. These transmissions can be scheduled often enough to disrupt all other communications. It is also called scrambling.
3) Reactive Jamming Attack: In which an attacker transmits a signal whenever it detects that another node has initiated a transmission, causing a collision during the second portion of the message.

MAC Layer

MAC layer incorporates functionality uniquely designed to the ability to discover networks, join and leave networks, and coordinate access to the radio medium. Possible DoS attacks are given below:
1) MAC Misbehavior
DoS attack can be implemented via corrupting CTS / RTS frames.
a) Unprompted CTS Attack
An attacker transmits a CTS message with a long message duration causing all recipients to halt transmission for this duration.
b) Reactive RTS Jamming Attack
Whenever a node detects an RTS message, it disrupts these messages by immediately initiating a transmission. The effects of this attack are exacerbated by the exponential back-off scheme.

c) CTS Corrupt Jamming
Upon receipt of a RTS message, an attacker transmits noise during the CTS response.

2) Selfish attack
The selfish nodes will reduce the resource of Wireless channel which can be used by legitimate nodes, thereby affect the network performance, and even interrupt the network service. There are two categories of selfish nodes in WMN, selfish client nodes and selfish router nodes. Selfish client nodes access WMN with selfish strategy to achieve greater throughput, reduce power consumption and improve QoS. Selfish router nodes use selfish strategy top result in the congestion of network or even the denial of service. With the characteristics of multi-hop and public access, it is more vulnerable for WMN to selfish client nodes attack. The selfish attacks in router nodes will also have significantly impact on the entire network performance.

Routing Layer

1) Blackhole Attack: In this attack, the malicious nodes broadcast itself as most optimal node for data forwarding. The malicious nodes then drop packets and hence deny the service.
2) Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.
3) Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.
4) Energy consummation: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.
5) Information disclosure: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.
6) Greyhole attack:
This attack is a small variation from the Black hole attack. In opposition to the Black hole attack, Greyhole routers (malicious nodes) do not drop all the packets just drop selective packets.
7) Wormhole attack:
In a wormhole attack, an attacker receives packets at one point in the network, "tunnels “them to another point in the network in order to create a shortcut (or wormhole) in the network through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker, and then replays them into the network from that point. The malicious node can use this position to maliciously drop packets in order to deny the services in the WMN.
8) Jellyfish attack:
It is done by complying protocols for packet dropping in malicious way to deny the services.
9) Byzantine attack: Attacks where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine attacks.
10) Sybil attack:
A Sybil attack is essentially an impersonation attack, in which a malicious device illegitimately fabricates multiple identities, behaving as if it were a larger number of nodes (instead of just one). Malicious device additional identities are referred to as Sybil identities or Sybil nodes.

11) Flooding attack: The attacker transmits a flood of packets toward a target node or to congest the network and degrade its performance. A flooding DOS attacks are difficult to handle. Attacker may use any type of packets to congest the network.

V. CONCLUSION

After reviewing the various attacks in MANET in depth, we believe that there will some difficulties in framing and performing various operations in the environment of wireless networking. It is true that performance suffers as the number of devices grows and large ad-hoc networks become difficult to route and manage. However, much time and more security is being devoted to achieving routing stability, and a few technical issues need to be solved before they become to a common place.

VI. ACKNOWLEDGEMENT

We extend our heart-felt gratitude to the management of SNS College of Technology (Autonomous) and The Principal Dr.S.Chenthur Pandian to carry out our Research Activities. We highly grateful to our guides; Dr.S.Karthik (Dean/CSE) and Dr.T.Kalaikumaran (HOD/CSE) for their valuable suggestions and guidance for our research work. We also extend our thanks to Our HOD Dr.L.M.Nithya for her plausible support.

REFERENCES

[1] Asleen Arora, Paramjeet Singh and Shaveta Rani ”Detecting and Preventing Attacks in MANET ”International Journal of Computer Applications ,Volume 81 - Number 5 ,2013.

[2] Priyanka Goyal, Vinti Parmar, Rahul Rishi,” MANET: Vulnerabilities, Challenges, Attacks, Application” IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[3] Aarti, Dr.S.S.Tyagi” Study of MANET: Challenges, Application and Security Attacks ” International Journal of Advanced Research in Computer Science and Software Engineering volume 3, Issue 5, May 2013, ISSN: 2277 128X.

[4] G. S. Mamatha, Dr. S. C. Sharma” Analyzing the MANET variations,Challenges,Capacity and protocol issues ” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[5] Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul Ghafoor Memon, Abdul Baqi” Denial of Service Attacks in Wireless Ad hoc Networks” Journal of Information & Communication Technology Vol. 4, No. 2, (Fall 2010) 01-10.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei” A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 2006 Springer.

[7] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma” A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks” Journal Of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[8] Reshmi Maulik, Nabendu Chaki” A Study on Wormhole Attacks in MANET” International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.

[9] Gagandeep, Aashima, Pawan Kumar” Analysis of Different Security Attacks in MANETs on protocol Stack A-Review” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[10]S Karthik, S Kannan, ML Valarmathi, VP Arunachalam,T Ravichandran”An Performance Analysis And Comparison Of Multi-Hop Wireless Ad-Hoc Network Routing Protocols In Manet ” Volume2,Issue4. International Journal of Academic Research, 2010

[11]K.P.Manikandan,Dr.R.Satyaprasad,Dr.K.Rajasekhararao, ”A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks ”International Journal of Advanced Computer Science and Applications(IJACSA), Volume 2 Issue 3, 2011.

[12] Puneet Kansal, Nishant Prabhat , Amit Rathee, ”Black hole attack in Manet ”International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013,SSN: 2277 128X.

[13]Ash Mohammad Abbas,Øivind Kure,“Quality of Service in mobile ad hoc networks*:* a surveys ”Int. J. Ad Hoc and Ubiquitous Computing, Vol. x, No. x, xxxx.

[14] M. Vijaya Lakshmi,Dr. S. Venkatachalam, ”Comparative analysis of QoS routing protocols in MANETS:Unicast &Multicast ”International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459,Volume 2, Issue 4,April2012)

[15] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008, ISSN: 2277 128X.

[16] M. Vijaya Lakshmi,Dr. S. Venkatachalam, ”Comparative analysis of QoS routing protocols in MANETS:Unicast &Multicast ”International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459,Volume 2, Issue 4,April2012

[17] M.Udhayamoorthi, C.Senthilkumar,Dr.S.Karthik, Dr.T.Kalaikumaran” A review on layers based attacks in MANET”NCNICS’14 Conference proceedings,March2014,Page no.94.