ISSN:0975-9646

Survey of MANET Attacks, Security Concerns and Measures

Shweta Jadye
Computer Science and Engineering Department, Career Point University
Kota, Rajasthan, India

Abstract **– Due to the fast changing scenario in field of wireless networking, MANET has emerged as a most promising area of research. MANET is self-organized network of mobile nodes with continuously changing topology. MANET has wide range of applications like military, rescue operations during natural calamities, commercial sectors, local level network/PAN etc. Due to basic characteristic of being ad – hoc, MANET is more prone to attacks. In this paper we will take a brief overview of several routing protocols, Attacks in MANET at different layers, and possible security measures.**

Keywords **– MANET, Routing protocols, Security attacks, IDS.**

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are infrastructure less networks with distributed operations [2]. Every node in MANET is free to enter or leave the network. In MANET all terminals are autonomous and use multi hop routing. In MANET mostly the nodes have low battery and small memory. As there is no central authority or access point in MANET, routing is very crucial issue. We have three approaches for routing in MANET and wide range of routing protocols [1]. Every protocol has its own advantages and limitations. We can list few weaknesses of MANET as – Limited bandwidth, low battery power, computational power, security etc. Research is going on to overcome all such issues. Out of these we are focusing more on security attacks in this paper.

In this paper firstly we will discuss why MANET is more disposed to security attack and what different types of attacks known till. Then we will discuss the available preventive measures.

II. REASONS OF MANET BEING UNSAFE

A. No central management – Every node in MANET is self-configured and self-administered. Therefore it is difficult check or control the transfer of data.

B. Freedom for a node – Any node in network is free to enter or leave the network so any malicious activity by a node cannot be tracked completely.

C. Low Power – In a MANET every node is light weighted so with small battery backup and small memory size.

D. Data loss during transmission – as both sender and receiver node are mobile there are frequent path breaks in MANET so possibility of data loss during transmission is high.

E. Limited bandwidth – Wireless network has much less capacity as that of wired network.

F. Trust issues with routing protocols – As every node in MANET is independent, routing protocols assumes that all nodes present in network are non-malicious and cooperative.

III. ROUTING PROTOCOLS

Routing protocols are mainly divided into three categories.

Proactive	Reactive	Hybrid[11]
•DSDV •GSR •CGSR •WRP •FRP	•DSR •TORA •ABR •AODV •SSR	•ZRP •HWMP •ZHLS

- Proactive protocols are also called as table driven as routing table is maintained throughout the process of communication, which sometimes leads to network overhead.
- Reactive protocols are on demand protocols. Routing information is sent to neighbors only if requested.
- Hybrid protocols make combination of both proactive and reactive techniques.

IV. SECURITY GOALS

For protecting data as well as resources from various attacks following security goals should be ensured [9].

A. Confidentiality – Data which is being transferred should only be read by the sender and receiver. No other in between node should get hold of the information which is being sent. This can be achieved by encrypting data.

B. Authentication – Data should be transferred only to the authenticated node.

C. Integrity – Integrity ensures that data is not modified during the communication by any malicious node.

D. Availability – All the network services should be available during data transmission. Though the attack happens system should be capable of providing required services.

V. SECURITY ATTACKS IN MANET

In MANET every mobile node works as a router whose work is to discover and maintain the routes within the network for data transmission. It is the responsibility of a node to find the shortest path between two nodes. That is why routing is very crucial and routing attacks [4] is the interest area of researchers.

A. Attack Categories -

Based on the domain and nature of the attacks we can generally divide attacks in following categories.

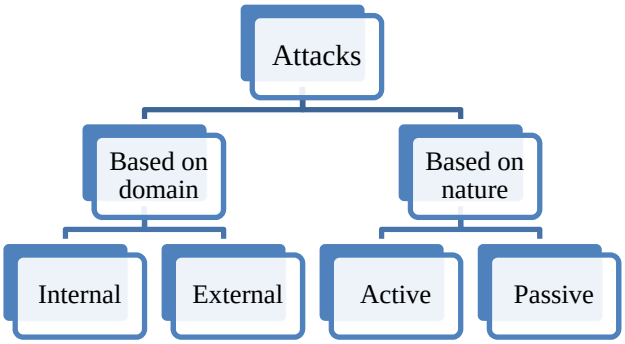

Fig.1 Categories of attacks

1) *Based on domain* –
   a) *Internal attack* – attacker is within the network i.e. any node in MANET is malicious
   b) *External attack* – Attacker attacks from outside of the network mostly the unknown entity or node.
2) *Based on nature* –
   a) *Active attacks* – It is an attempt to modify or alter the data without proper authority. It may also include inserting false packets into main data stream to gain the authorization. Attacks in this category can further divided into internal or external attack.
   b) *Passive attack* – Such attacks does not interrupt the function of routing protocol but it tries to gathers the confidential information by listening to the traffic. Such types of attacks are difficult to trace.

Some research is done based on attacks on various layers in protocol stack [12]. We can summarize the attacks as shown in below.

B. Summary of attacks -

- Eavesdropping - Attacker reads data packets. It happens at physical layer.
- Jamming - It is a kind of DoS attack. Pulses or noise are introduced in network.
- Block hole - Attacker gives false routing information and directs whole traffic to itself. It imitates as having optimal path and drops the packet received. It is network layer attack.
- Worm hole - It is also called as tunneling attack. Confidential information is transferred between two malicious node by interpreting as neighbors. In such category of attack multiple malicious nodes work together.
- Gray hole - It is same as black hole attack but in this kind of attack attacker sometimes drops the packets and sometimes behaves like normal node.
- Link spoofing - Attacker advertise as being two hop neighbor with fake links and manipulate data.
- Rushing - Whenever attacker receives RREQ it floods the network and try to immitate as the real source.
- Flooding - Network is flooded with false roting information by malicious node and consumes network resources. It is also called as resource consumption attack
- Sybil - Attacker shows multiple identities of many target nodes and data packets are redirected to the attacker.
- Byzantine attack – In this attack one or more compromised nodes works together to create loops in routing path or such nodes forwards the packets on the non-optimal paths thus affecting the QoS.

Based on the attack patterns few case studies [10] are prepared. This study suggests different techniques like one way hash function(for DSDV), MACs and shared keys for authentication(for DSR), Inverse priority ranking(SRP), Public key cryptography(ARAN) etc.

VI. Problems Faced due to Attacks

While discussing different attacks it is necessary to consider problems occurred due to various attacks. Due to different attacks at different layers we face following problems

A) Time delay – Any type of attack leads to time delay in a network. This may further lead to rejecting/discarding the request by receiver.

B) Loss of data – Attacks like Black hole attack, gray hole attack malicious node attracts traffic by giving incorrect routing information and drops all/some data as well as control packets passing through it. In such cases complete or partial data loss occurs.

C) Fully/Partial paralyzing the network – In the case of Fabrication attack, modification attack when the link is broken or routing table of nodes are destroyed with faulty information then there is a possibility of paralyzing the network[8].

D) Compromise QoS – Attacks like tunneling or worm hole attack compromise the security of network. In such cases packet is forwarded to a node which is at multi hop distance through a tunnel and redirect back to network[10]. In such case the other might get whole information about network thus QoS is affected.

E) Misuse of services – When any node make a selfish behavior it tends to misuse the services provided by MANET. Like consuming bandwidth and flood the network.

VII. Attack Detection and/or Prevention Mechanism

Identifying an attack in MANET is not very easy because most of the time attacker is internal node and routing protocol believes that every node in the network is trustworthy. One more thing is to be considered while applying the detection technique is which routing protocol is being used. There is a lot of work done in detection and/or prevention techniques. This study is summarized below for few routing protocols.

A) Detection techniques - Intrusion detection system (IDS)

There are various techniques to find out malicious or selfish nodes [24]. Intrusion detection system are placed in MANET to monitor the network for any malicious activity.

1) Standalone IDS – In this scheme every node in MANET has its own IDS and monitors the activities performed by the node.

2) Cluster based IDS – Multiple nodes form a cluster and IDS monitors the activity of the cluster.

3) Zone based IDS - IDS is placed based on zonal nodes. Nodes are divided into different zones based on geographical information.

An IDS works based on following techniques [19]-

1) Anomaly based - In anomaly based IDS normal behavior of network is extracted and every activity is checked against it.

2) Misuse-Based - In Misuse based IDS system can store a signature of intrusion in a database and compare every time with an ongoing activity. This IDS works efficiently but fails for new attack.

3) Specification-based - In specification based IDS, a set of specification are already designed for the network and all ongoing activities are checked against it.

Few extensions are also provided for above mentioned detection systems like EAACK-A Secure Intrusion Detection System for MANET [26] – It uses secure acknowledgment and misbehavior report authentication. Digital signature used in this IDS prevents false acknowledgement packets.

There are various algorithms and detection schemes are discussed in [9] like Core, confidant, Watchdog and pathrater.

B) Security Measures – As there are multiple threats at different layers it is important to provide security mechanism at the time of routing. There are various measures taken at different levels to ensure security.

Many protocols or schemes are discussed in [17] against black hole attack, wormhole attack and gray hole attacks. As well as few measures are suggested against flooding attacks, rushing attacks, DoS attacks. Commonly suggested mechanisms are

1) Security by cryptography – An authentication scheme should be provided for routing. As well as cryptography can be used for secure routing. [4].

2) Change in format of routing information – Few extra fields are used to maintain the information about neighbors. This is to ensure that the neighbor is not a malicious or selfish node.

3)Trust based forwarding scheme [25] – In this scheme a trust counter is associated with every node. While routing packets a hash value is also forwarded to destination node. If the received hash value is verified by destination node then the trust counter is incremented else decremented. Thus if the trust counter is decreased below the threshold value , it will be treated as malicious activity.

If we further classify the detection schemes according to attack we can summarize few as follows

a) Detection schemes for Black hole attack - Few methods are discussed in [30] for detection and prevention of Black hole attacks in AODV based network. These measures include watchdog timer, monitoring the tables of neighbors (local collaboration), Cross checking incoming routing packets from neighbors (cross validation), Setting a limit for sequence number etc.

Enhanced route discovery scheme(ERDA) [29] proposes few changes in routing table of AODV and in updating process.

Same paper [29] suggests ABM(Anti Black hole Mechanism) scheme in which suspicious value of a node can be identified based on the difference between request and reply sent from node. If this suspicious value is very high then black hole attack can be identified.

In another security approach [28] every node in network maintains a black identification table(BIT) and packet modified count(PMC). Based on the information from BIT of neighbor nodes, PMC is updated. If node is malicious then received data is different from original. Here another table, isolation table(IT) is maintained and malicious node is added to ID.

Another method of invalid IP addresses is suggested in [28] for the detection of black hole attack. In this method every node is assigned with one valid and one invalid IP address. If all nodes are working fine they will just forward the packet coming from invalid address but a malicious node will send a reply to invalid IP address suggesting that its having an optimal path. Thus a black hole attack is identified and such node will be isolated.

b) Detection schemes for Gray hole attack – Based on the data routing information (DRI) table a method is proposed in [32]. In this method each node maintains a DRI table for neighbors. If there is not any entry for any node which is present in network then anomaly based detection is done for such node. If node is found malicious then this information is forwarded in whole network.

Various methods are also suggested in [30] which also work well for black hole attack. Such methods include watchdog timer, checking the reply sequence number with threshold value, Behavior checking by strong nodes in the network etc.

c) Detection schemes for Byzantine attack – Various security schemes are discussed in [34] against byzantine attacks. It includes channel aware detection algorithm which identifies selective forwarding, hash function based method which generates behavioral proofs based on data traffic and forwarding paths, DCIID algorithm using packet verifiers, Cooperative detection mechanism etc.

An IDS is introduced in [35] for detecting byzantine attack in AODV. In this scheme IDS monitors the network profile before the entry of node and after the exit of node. If profile change is detected by IDS it is treated as attack.

A game theory [36] is also proposed in attack defense system to detect byzantine attack. This theory is of great help within the environment with large number nodes.

VIII. CONCLUSION

In this paper we have discussed different types of security attacks in MANET. Also we have studied different security measures suggested for detection and prevention of few attacks in MANET like Black hole attack, Gray hole attack, Byzantine attack. All the methods surveyed for this paper have suggested few changes in the routing protocols. Based on this survey it can be suggested as there is a lot more scope in the field of attack detection and prevention schemes for MANET.

REFERENCES

[1] Nawneet Raj, Priyanka Bharti, Sanjeev Thakur, "Qualitative and Quantitative Based Comparison of Proactive and Reactive Routing Approaches in MANET ", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.12, December- 2015, pg. 177-184

[2] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks" IJARCSSE, Volume 3, Issue 5, May 2013

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

[4] Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim,"Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", 15th International Conference on Computer Modelling and Simulation

[5] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine • October 200270

[6] 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

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" WIRELESS/MOBILE NETWORK SECURITY, Chapter 12

[8] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah," SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY", IJCSES Vol.6, No.1, February 2015

[9] Parul Tomar et. al "A Comparative Study for Secure Routing in MANET" International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010

[10] Ashwani Garg, Vikas Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", IJERCSSE, Volume 2, Issue 9, September 2012 ISSN: 2277 128X

[11] Apoorva Chandra, Sanjeev Thakur," Qualitative Analysis of Hybrid Routing Protocols Against Network Layer Attacks in MANET", IJCSMC, Vol. 4, Issue. 6, June 2015, pg.538 – 543

[12] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", IJEAT, ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[13] Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection" (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011

[14] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011, 1:4

[15] Imrich chlamtac, Marco Conti, Jennifer J.-N.Liu, " Ad Hoc networks 1 (2003)

[16] Manjeet Singh, Gaganpreet Kaur "A Surveys of Attacks in MANET", IJARCSSE, Volume 3, Issue 6, June 2013

[17] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "DoS Attacks in Mobile Ad-hoc Networks: A Survey", 2nd International Conference on Advanced Computing & Communication Technologies2012

[18] Jiejun Kong, Xiaoyan Hong, Mario Gerla, "A NEW SET OF PASSIVE ROUTING ATTACKS IN MOBILE AD HOC NETWORKS"

[19] Adnan Nadeem, Member, IEEE, and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013

[20] Swarnali Hazra, S.K.Setua, "Sybil Attack Defending Trusted AODV in Ad-hoc Netwok" , 2nd International Conference on Computer Science and Network Technology 2012

[21] Ketan S. Chavda, Ashish V.Nimavat, "REMOVAL OF BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL OF MANET", 4th ICCCNT - 2013

[22] Yinghua Guo, Steven Gordon, Sylvie Perreau, "A Flow Based Detection Mechanism against Flooding Attacks in Mobile Ad Hoc Networks", WCNC 2007 proceedings.

[23] Himadri Nath Saha , Dr. Debika Bhattacharyya, Dr. P. K.Banerjee, Aniruddha Bhattacharyya ,Arnab Banerjee, Dipayan Bose, "STUDY OF DIFFERENT ATTACKS IN MANET WITH ITS DETECTION & MITIGATION SCHEMES", IJAET/Vol.III/ Issue I/January-March, 2012/383-388

[24] Martin Schütte, "Detecting Selfish and Malicious Nodes in MANETs", seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, sommersemester 2006

[25] A.Rajaram, Dr. S. Palaniswami, "Malicious Node Detection System for Mobile Ad hoc Networks" IJCSITVol. 1 (2) , 2010, 77-85

[26] K.Chinthanai chelvan,T.Sangeetha,V.Prabakaran,D.Saravanan, "EAACK-A Secure Intrusion Detection System for MANET" IJIRCCE Vol. 2, Issue 4, April 2014

[27] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", ternational Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[28] Reza Amiri, Marjan Kuchaki Rafsanjani2 and Ehsan Khosravi, "Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks", Indian Journal of Science and Technology, Vol 7(4), 401–408, April 2014

[29] Bhoomika Patel, Khushboo Trivedi, "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET", IJCSIT, Vol. 5 (3) , 2014, 2816-2818

[30] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi, "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[31] Poonam Rani , Neeraj Garg, "SURVEY PAPER ON BLACKHOLE DETECTION SCHEMES IN MANET", IJERAT Vol. 2, Issue IV, April 2014

[32] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar," A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", ICICS 2007

[33] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", IJCA Volume 53– No.16, September 2012

[34] Neha Mahajan, Rajeev Bedi, S. K. Gupta, "A Survey on Detection of Byzantine and Resource Consumption Attacks", Journal of Basic and Applied Engineering Research Volume 1, Number 7; October, 2014

[35] Neha Agrawal, Krishna Kumar Joshi, Neelam Joshi, "Implemented and Evaluated the Byzantine Attack with the Aid of Rushing Attack in Manet" , IJCA Volume 130 – No.6, November2015

[36] Ms.Chetna Guntewar, Mrs. Vaishali Sahare, "A Review on Byzantine Attack Detection and Prevention Using Game Theory", IJCSIT Vol. 6 (1) , 2015, 749-752

[37] Er. Nitin Mohil, Ms. Kanta Dhankhar, "Survey of Detection and Prevention Mechanism for Flooding Attacks in MANETs", International Journal of Research in Advent Technology, Vol.2, No.5, May 2014

[38] Bhuvaneshwari .k, Dr. A. Francis Saviour Devaraj, "PDS-AProfile based Detection Scheme for floodingattackin AODV basedMANET", International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 3, June 2013