ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY OF VARIOUS SECURITY ATTACKS IN MANETS

Pooja Rani*, Prabhpreet Kaur
* M.Tech,Department of Computer Science, Guru Nanak Dev University, Amritsar, India
Assistant Prof.,Department of Computer Science, Guru Nanak Dev University, Amritsar, India

ABSTRACT

Mobile Ad hoc network (MANET) is considered a gathering of wireless portable nodes that are accomplished of shared with each other without the usage of a network infrastructure. MANET is mostly weak due to its essential features, such as undeveloped peer-to-peer manner, shared wireless medium, harsh source restrictions, greatly lively network topology and nodes openness to bodily detention. Security is most important facility for all kind of network communications. MANET should provide safety that grows people's confidence on MANET. In this paper a survey on MANET attacks are presented. This helps to understand different types of attacks and how they affect the act of network.

KEYWORDS: MANET, Protocols, Attacks, Security etc.

INTRODUCTION

Mobile Ad-hoc networks stand the infrastructure less wireless links, i.e. there is no central power and the nodes are mobile therefore the topology of network is lively in nature [3]. There are many use areas of MANETS like military processes, rescue processes during any natural disaster, emergency services and cellular headsets. MANETs have many features connected with them like ad-hoc in nature, easy and quick to implement, easy to sustain, economical (eliminates cabling cost). Wireless networks have different features, applications and needs than conventional wired network. Consequently traditional routing protocols can't be used to facilitate communication among mobile nodes. Moreover MANETs are open media in nature (there is no network boundary). As a result we need to have different routing protocols for such networks [7]. Routing protocols popular MANET can be broadly considered as follows: *Proactive routing protocols* are table driven protocol like DSDV. *Reactive routing protocols* are on request protocols like AODV, DSR etc. *Hybrid routing protocols*: There is a trade-off among proactive and reactive protocols like ZRP, LANMAR etc.

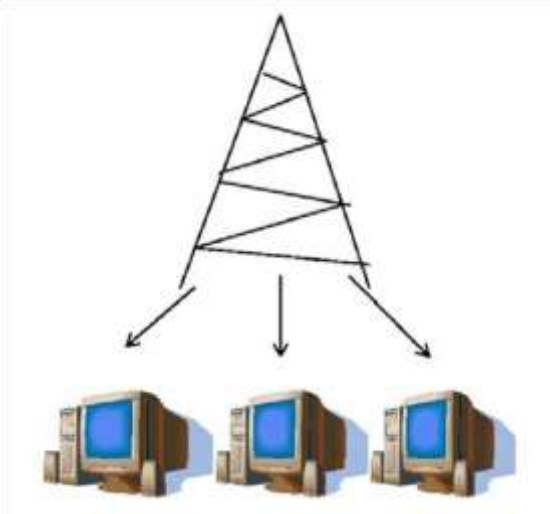

Figure 1: Infrastructure based networks

VULNERABILITIES IN MANET

Routing protocols linked to MANET lack two features viz. security (since there is no central authority) and cooperation (since nodes are mobile and may behave selfish at times). Conventional security outputs opted for wired networks fall ineffective and inefficient for wireless networks [2]. Hence to get security outputs for these networks we need to take in mind their vulnerabilities such as:

1. Dynamic topology*:* In addition to the absence of any network boundary, the interconnected nodes are mobile in nature. Consequently the topology of network keeps modifying which makes it even harder to distinguish the normal behavior of network from cruel.
2. Wireless links connecting the nodes: Since radio waves or other wireless links are opted to interconnect the nodes forming a network, it creates the network liable to attacks such as interference (active) in addition to eavesdropping. Also attackers may consume network bandwidth.
3. Cooperation*:* Routing algorithms in MANET supposed that all the knobs are non-malicious and cooperative in nature consequently the attacker can simply become a routing agent and affect the network topology and actions.
4. Absence of network boundary*:* There is no clear line of protection that differentiate the network from outside world. 5. Restricted resources*:* MANET may consist of variety of shared devices like mobile phones, PDAs, laptops etc. these devices may have different storage and computing ability. Battery of shared devices is the main resource in case of MANET that must be taken care.

RELATED WORK

In[1] W.Bing et.al(2006) has discussed, Rushing attacks are primarily beside the on request routing protocols. Rushing attack preclusion (RAP), generic rushing attack anticipation appliance introduced for the reactive protocols. In[2] F. Anjum et.al(2007) has proposed, (DoS) distributed denial of Service attacks on the Internet. Studied several security matters in MANET and conferred the possessions of distributed denial of service attacks on MANET or network routine. In [4] C. Siva Ram Murthy et.al(2009) has discussed, Impact of Wormhole attack is affected the throughput of packet ratio in positions of packet received, packet sent and packet drop. In 5] U.Saurabh, et.al(2011) has discussed ,A Replay attack is a procedure of network attack in which a effective data transmission is meanly or falsely frequent or delayed. In [6] S.Laxmi, et.al(2011) has proposed, In Snooping attack, an attacker can also change the messages creating from other nodes formerly relaying them. [10][11] D.Rajib, et.al(2014) has proposed, Black hole affect the throughput and packet ration of the network.it decreases the quantity of the network and packet drop ratio increases after black hole attack. In[8] S.Mojtaba et.al(2013) has discussed, about Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack.

TYPES OF SECURITY TYPES PROPOSED IN MANET

Security in Mobile Ad-Hoc Network (MANET) is the greatest significant worry for the simple functionality of network. Accessibility of network facilities, privacy also reliability of the records can be realized by declaring that safety matters have been seen. MANET regularly writhe from safety attacks because of its structures similar undeveloped medium, altering its topology dynamically, lack of significant nursing and management, supportive algorithms and no clear defense mechanism[12]. These features have altered the conflict field condition for the MANET Different types of attacks in MANET are simplified below:

Internal vs. External Attack

- Internal attack-These attacks are caused through cooperated nodes, which are the portion of our network.
- External attack- These are passed out by the nodes that do not belong to the area of our network.

Active vs. Passive Attack

- Active attack-Attacker tries to alter the data being replaced over network and may disrupt normal working of network. It may also inject, drop or alter the packets.
- Passive attack-Attacker just snoops the data exchange over network without altering it. This attack targets confidentiality. It is hard to detect, easy to introduction and may lead to active attacks.

ATTACKS AGAINST ROUTING LAYERS IN MANET

The attacks, which MANET is prone to, might have the aim of adjusting the routing protocol so that traffic runs over a particular node which is measured through the attacker. Attacks on the routing level can be categorized into two main classes: inappropriate traffic generation and inappropriate traffic relaying.

Inappropriate Traffic Generation
This attack includes transfer wrong control messages, i.e. control messages directed in place of additional node (identity spoofing), or control messages which contain wrong or outmoded routing information. This attack leads to reduction in network transportations, unapproachable nodes, and probable routing loops.

Snooping
In [6] have proposed, it is unauthorized access to someone's personal data. It may include watching someone while typing or observing some other person's e-mail. In more refined snooping, the attacker uses software series to remotely observe a computer device. Malicious hackers often use this technique in order to capture login information by snooping the key strokes.

Byzantine Attack
In [12] have proposed, this attack, a set of nodes work in involvement and performs malicious functions like generating routing loops, progressing the packets to non-optimal paths, selectively dropping of packets etc. This attack is very tough to detect.

Message Bombing
In [6] have proposed, the attacker can also attempt to achieve Denial of Service on the network layer through drenching the medium through a storm of broadcast messages. The attacker may also send unacceptable messages just to retain nodes engaged, homicide their CPU cycles and draining their battery influence. In this case the attack is not pointed at modifying the network topology, but rather at generally disturbing the network functions and communications..

DoS Attacks
In [2] have proposed, DoS attacks make a networked system or facility unattainable toward legimates users. These outbreaks are an infuriation on bottom, or can be really destructive if a serious structure is the main target. Damage of network assets origins commercial misplacement, work delays, and loss of communication among network users. Output necessity be produced toward avoid these DoS attacks. In this paper, discoursed distributed denial of service attacks on the Internet. Revised several safety matters in MANET and discussed the possessions of distributed denial of service attacks on MANET or network act.

Inappropriate Traffic Relaying
In[6] have proposed, this attack the network communications coming after authentic, protocol-compliant nodes can be corrupted through improper nodes, which then spreads all over the network and hence affects the network performance.

Message Tampering
In [6] have discussed, an attacker can also change the messages creating from additional nodes before relaying them, if a mechanism for message integrity is not utilized properly.

Replay Attack
In [5] have discussed, a Replay attack is arrangement of system attack in which effective data transmission is meanly otherwise falsely frequent or overdue. That is passed out either through the creator who captures the data and retransmits it, maybe as portion of a pretense attack by IP packet replacement. However some of the countermeasures are time stamping, one-time passwords and session tokens. An attacker observing old effective control messages and re-sending them through a replay attack, by this other nodes change their routing table through false routes. This attack is fruitful even if control messages allow a résumé or a digital signature that does not contain a timestamp.

Rushing Attack
In [1] have proposed, Rushing attacks are primarily beside the on request routing protocols, where the nodes must progressed to the main established Route Request from every route finding; completely additional received Route requests are unnoticed. The attack contains, for the opponent, in rapidly sending its Route Request messages when a route finding is begin. If the Route Requests first grasp the target's point are those of the attacker, then some located route contains the attacker. Rushing attack can be achieved by weak attacker and it outputs in denial in service attack and it is harmful attack. Therefore a Rushing attack prevention (RAP), generic rushing attack preclusion appliance presented for the reactive protocols.

Worm hole Attack

IN [4] they have discussed Wormhole attack is a very strong attack that is created by malicious colluding nodes. It does not require any cryptographic worn out. The wormhole attack is a strong attack that can have thoughtful significances on many suggested ad hoc network routing protocols. An attacker who can organize a successful wormhole attack can corrupt routing, deny service to large segments of a network, creation of not connected component within a network. In this paper we have discussed the several ways by which the wormhole can be handled. Results said that impact of wormhole attack affect the packet delivery ratio and throughput.

Table 1.Impact of Wormhole Attack.

No. of Nodes	Attack Name	Parameter	Attack Type	Without attack	With Attack
50	Worm hole	Packet drop ratio	active	40	170

Black hole Attack

In [9] [10] [11] have proposed the black hole attack which can be straddling beside a MANET and suggested possible result used for it in the AODV protocol. The suggested result can be implemented to Identify for single and multiple black hole nodes collaborating by every other in a MANET and also finds safe routes from source to destination through avoiding multiple black hole nodes acting in collaboration. Impact on packet delivery ratio and throughput also noticed. They observe that throughput and packet delivery ratio is also decreased.

Table 1.2 Impact of Black hole Attack.

Protocol	**Attack Name**	**Attack Type**	**Parameter**	**Without attack**	**With attack**
AODV	Black hole	Active	Packet delivery ratio	100	90
AODV	Black hole	Active	Throughput	98	70

RESULTS AND CONCLUSION

In this paper, I studied about various types of security attacks in MANET to see its effect on MANET using different routing protocols. NS2 simulator is used and we compared performance of different security attacks on different protocols based on certain parameters like PDR, Average throughput, average end to end delay etc. Due to the mobility and exposed media nature of MANET these networks are more disposed to security fears as associated to the wired network. I saw that the these attacks effects the network performance which can be analyzed using various network parameters like total packets sent, total packets received, throughput, packet delivery fraction by the help of simulation and graphs, etc. Consequently security needs are higher in MANET as compared to the traditional network. Hence I need a secure and reliable routing protocol that can be fastly deployed and follows dynamic routing. AODV is prone to many attacks similar spoofing, fabrication of error messages, source route tunneling, modification in sequence no. and hop count etc.

Table 1.3 Comparative analysis of different security attacks based on certain parameters on different protocols in MANET [8][15].

No. of Nodes	**Attack Name**	**Attack Type**	**Layer**	**Protocol**	**Average Packet delivery ratio**	**Average Throughput**	**Average End to end delay**
100	Black hole	Active	Network	AODV	90	80	0.5
100	Black hole	Active	Network	ZRP	45	350	0.4

100	Black hole	Active	Network	OLSR	25	40	0.5
100	Black hole	Active	Network	DSR	28	75	0.25
30	Worm hole	Active	Network	AODV	0.1	0.4	7
30	Worm hole	Active	Network	DSR	0.2	0.6	30
16	Denial-service	Active	Physical	AODV	-	480	0.000055
16	Denial-service	Active	Physical	OLSR	-	490	0.000058
16	Denial-service	Active	Physical	GRP	-	190	0.00006

REFERENCE

[1] Bing Wu, Jianmin Chen and Jie Wu, and MihaelCardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer©, PP. 1-38, 2006.
[2] F. Anjum and P. Mouchtaris, "Security for Wireless Ad Hoc Networks", Wiley-InterScience, New York, NY, USA,
[3] Preeti, YogeshChaba, and Yudhvir Singh, "Review Of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET", National Conference on Challenges and Opportunities in Information Technology, PP.56-59, 2008.
[4] C. Siva Ram Murthy and B.S. Manoj, "Ad-Hoc wireless networks", Architecture and protocols, Pearson Education, Fourth Impression, 2009.
[5] SaurabhUpadhyay, and Brijesh Kumar Chaurasia, "Impacts Of Wormhole Attacks On MANETs, International Journel of Computer Science and Emerging Technologies", Volume 2, Issue 1, PP.77-82, Feb 2011.
[6] LaxmiShrivastava, Sarita S. Bhadauria and G.S. Tomar, " Performance Evaluation of Routing Protocols in MANET with different traffic loads", International Conference on Communication System and Networks Technologies, 2011.
[7] Vikas Kumar Upadhyay and Rajesh Shukla "An Assessment of Security attack over Mobile Ad-Hoc Network", Internal Journel on Advanced Networking and Applications, Volume: 05 Issue: 01, PP.1858-1866, 2013
[8] MojtabaGhanaatPishehSanaei, Ismail FauziIsnin and MajidBakhtiari, "Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack ",International Journal of Computer Networks and Communications Security,PP.1-6, VOL-1, 2013.
[9] Michalis Papadopoulos, Constandnos X ,GeorgiosSkourletopoulos and George Mastorakis and EvangelosPallis, " Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", International Conference on Telecommunications and Multimedia, PP.104-110, 2014.
[10] Rajib Das, and BipulsyamPurkayastha and Prodipto Das, "Security Measures For Black Hole Attacks in MANET: An Approach", PP. 1-7.
[11] KishorJyoti Sharma, Rupam Sharma, and RajdeepDas,"A Survey of Black Hole Attack Detection in MANET", International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT), PP.202205,2014.
[12] Rajakumar P, Prasannavenkatesan T and PitchaikkannuA,"Security Attacks and Detection Schemes in MANET ",International Conference on Electronics and Communication Systems(ICECS), PP.1-6, Feb.2014.
[13] Jasleen Kaur and Shakti Nagpal, "Review Paper on Security Challenges and Attacks in Mobile Ad-Hoc Networks ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, PP.1501-1508, May 2014.
[14] Wikipedia, "The free encyclopedia-, Mobile ad-hoc Network", http://en.wikipedia.org/wiki/Mobile_ad-hoc_network, Oct-2014.
[15] NeerajArora and Dr. N.C. Barwar, "Performance Analysis of Black Hole Attack on different MANET Routing Protocol ", International Journal of Computer Science and Information Technologies (IJCSIT), PP.4417-19, Vol. 5 (3), 2014.