DoS, Vampire, Probe, U2R Attacks in MANET Environment: A Review

Gurveen Vaseer[1], Pushpinder Singh Patheja[2].
Department of Computer Science and Engineering, OP Jindal University, Raigarh.[1]
Department of Computer Science and Engineering, VIT University, Bhopal.[2]

***Abstract*—**Mobile ad-hoc networks (MANETs) have gained immense popularity in the past few years with the growth in mobile devices, thus making them prone to malicious attacks and posing a threat to security. Attackers hamper the functioning of the network and hence need to be encountered to make the network flawless. In this paper we shall study the characteristics and threats caused due to for major attacks viz. Denial of Service(DoS), Vampire, Probe, User-to-Root(U2R).

Keywords-Attack, Probe, DoS, Vampire, U2R, MANETs, detection.

I. INTRODUCTION

MANET is a self-configuring network of mobile routers connected by wireless links with no access point where each mobile device in a network is autonomous. The mobile devices are free to move in any manner and organize themselves in a random fashion. Nodes in MANETs join and leave the network dynamically which shows their independent and self-deployable behavior [1], making them susceptible to attacks that affect the performance and functioning of the network.

Denial of Service(DoS) is a network attack that prevents or jams legitimate users from using a victim resource or computing device [2]. These attacks are posing a great threat to users and networks. Vampire attacks are not protocol specific; they tend to induce more energy drain that does not accomplish a possible solution hence making the network faulty [3]. Probe enables data capturing by gaining secret information in the network that violate confidentiality, messages can be deleted also by attackers. User-to-Root (U2R) is an attack in which an attacker accesses the account of normal users on a system and exploits some vulnerability that causes damage to the network [4].

II. RELATED WORK

Mobile Ad Hoc Networks (MANETs) correspond to the decentralized paradigms where clients themselves maintain the network in the absence of a significant infrastructure [5].
The work done by researchers in the past has been listed in Table 1 given below:

S.No.	Name of Authors	Work Done	Our Work
1.	A.Vincy, V.Uma Devi [6]	Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack	Analyzing all four attacks in detail.
2.	P. Kavitha, Rajeswari Mukesh[7]	To detect malicious nodes in the Mobile Ad-hoc Networks using soft computing techniques	Discussing the threats of all four attacks.
3.	Mamta Jha Rajesh Singh S.S. Dhakad[8]	Review of DoS attacks in MANET and the need for security	Analyzing all four attacks in detail.
4.	Harsha.N, Rashmi.S [9]	Detection of Vampire Attack and Prevention in MANET	Analysis of vampire attack
5.	Sheetal Panjeta, Er. Kanika Aggarwal [10]	Review of DoS, vampire, probe, R2L attacks	Analysis of DoS, vampire, probe, U2R

Table 1: Related Works

III. STUDY OF ATTACKS

MANETs are highly vulnerable to attacks which greatly decrease the network performance and its functioning drops hence posing a threat to users.

Attacks are mainly of two kinds:
1. Active attacks
2. Passive attacks

Active Attacks : This is the type of attacks in which fake data or information are inserted in to the network which harmful for network because the main aim of attackers tries to disturb the network performance like congestion, propagation of fake route information or modification or disruption etc. black hole attacks are the examples of these attacks.

Passive Attacks: This is the type of attacks in which extract the important information without modify or change the data packet in the network, this means attacker act as the intermediate node does not harm the network but only take the valuable information or knows about which type of communication are going on (between sender & receiver).Eavesdropping, traffic analysis, traffic monitoring and snooping are the examples of passive attacks.

Denial of Service attackposes a serious threat for adhoc networks. DoS does not only exhaust the system resources but also isolate legal users from the network.
The DoS attacks targets resources that can be grouped into three broad scenarios.

Figure 1 shows the scenario of DoS attack in MANET.

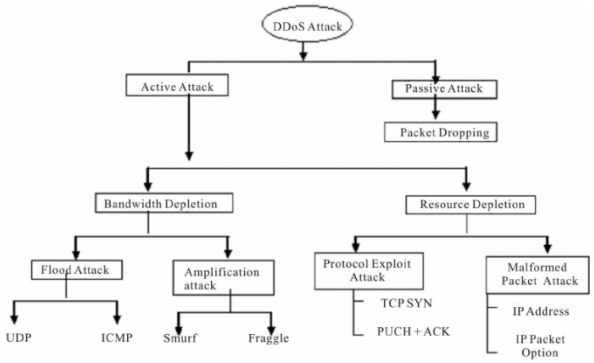

Figure 1

Challenges of DoS attacks:

The first attack scenario is a threat to Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Let us consider the case where a node continuously sends an executable flooding packet to its neighborhood and to overload the storage space thus to deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in MANETs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node.

The last scenario poses a problem to bandwidth. Consider the case where an attacker is located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations.

Vampire attack is a kind of attack which aims to make the network faulty by exhausting its resource capability. Here, the attacker communicates unimportant messages formally known as false packet to increase network traffic and make target node busy in useless activity.

Figure 2 shows the scenario of Vampire attack in MANET.

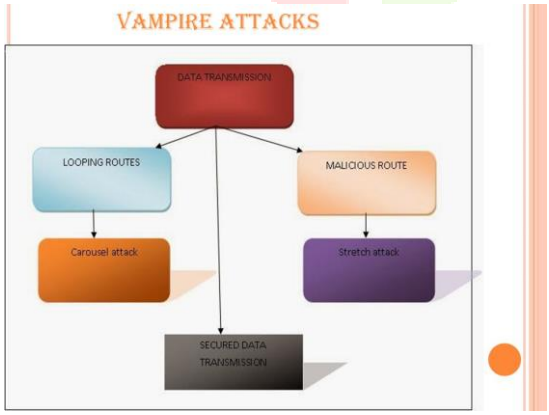

Figure 2

Challenges of Vampire attacks:

Vampire attacks are not protocol-specific, that is they do not depend on design properties or implementation faults of particular routing protocols, but exploit the general properties of protocol classes such as link-state, distance-vector, source routing and geographic and beacon routing. Their main aim is to drain the energy hence preventing a possible solution. Since Vampire attacks make use of protocol-compliant messages, their detection and prevention becomes very difficult.Each node is involved in routing by forwarding data for other nodes, so the finding of nodes that forward data is made in a dynamic manner on the basis of network connectivity.

Probing is a type of attack where attacker node scans the mobile device i.e. its capability, communication link watches and determines the vulnerability of the network so that in future he can exploit the network and capture the genuine data.

Figure 3 shows the scenario of Probe attack in MANET

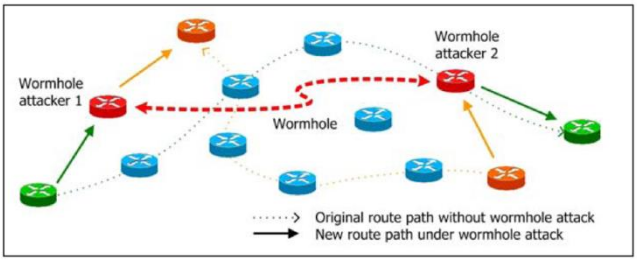

Figure 3

User to Root (U2R) attacks targets the super user of the system.They damage the operating system or application software of the particular system hence exploiting it. The attacker begins access to a normal user account on the system (by sniffing password, a dictionary attack or social engineering) and is able to exploit some vulnerability to gain root access to the system.

Figure 4 shows the scenario of U2R attack in MANET.

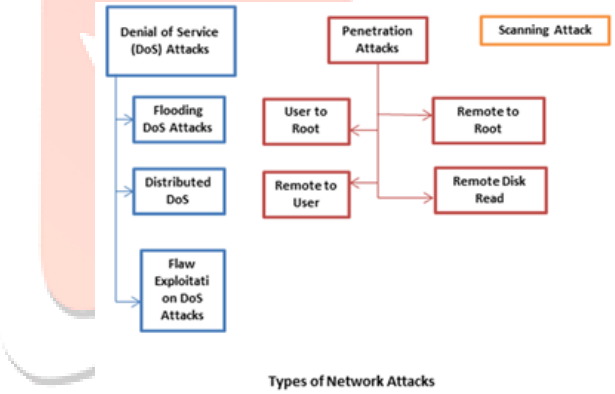

Figure 4

Challenges of U2R attack:

U2R attacks correspond to a local user on a machine gaining privileges normally reserved for the UNIX root or super user.

The U2R attacks leads to several vulnerability such as sniffing password, a dictionary attack and social engineering attacks.

The major attack in U2R is buffer overflow which copies too many data into static buffer without checking whether the data will exactly fit into program.

IV. CONCLUSION AND FUTURE WORK

In this paper we have studied various attacks associated with MANETs viz. Probe, Vampire, DoS and U-to-R attack. Their functioning and challenges that they pose to networks have been discussed in this paper. It is a review paper that throws light on the various issues of these four attacks and hence their detection and prevention becomes mandatory for a network.

REFERENCES

[1] Salim El Khediri ; Nejah Nasri ; Awatef Benfradj ; Abdennaceur Kachouri ; Anne Wei, "Routing protocols in MANET: Performance comparison

of AODV, DSR and DSDV protocols using NS2", IEEE, December 2014, p 1-4.

[2] Rajbir Kaur, M. S. Gaur, Lalith Suresh, V. Laxmi, "DoS Attacks in MANETs: Detection and Countermeasures", IGI Global, DOI: 10.4018/978-1-60960-123-2.ch010.

[3] Eugene Y. Vasserman, Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks, University of Minnesota.

[4] Shahid Anwar, Jasni Mohamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Suleman Khan, Bokolo Anthony, Victor Chang, "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions", Algorithms 2017, 10, 39; doi:10.3390/a10020039.

[5] Vidya.M and Reshmi.S," Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks,"International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1, Issue 1 (March 2014)

[6] A.Vincy, V.Uma Devi" Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack", IEEE International Conference on Innovations in Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[7] P. Kavitha, Rajeswari Mukesh, "To detect malicious nodes in the Mobile Ad-hoc Networks using soft computing technique", DOI: 10.1109/ECS.2015.7124851.

[8] Mamta Jha, Rajesh Singh, S.S. Dhakad, "A Review: Denial of Service Attack MANET", IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 01, 2015.

[9] Harsha.N, Rashmi.S, "Detection of Vampire Attack and Prevention in MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

[10] Sheetal Panjeta, Er. Kanika Aggarwal, "Review paper on Different Techniques in Combination with IDS", IJESC, Volume 7 Issue No.5.

[11] V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp.1333-1344, Aug. 1999.

[12] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[13] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002

[14] Susan Sharon George and Suma.R,"Attack-Resistant Routing for Wireless Ad Hoc Network", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.

[15] Gowthami.M, Jessy Nirmal.A.G, P.S.K.Patra3," Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks ", International Journal of Advanced Research in Computer Science & Technology Vol. 2 Issue Special 1 Jan-March 2014.

[16] Tripti Nema, Akhilesh Waoo, P.S.Patheja, Dr.Sanjay Sharma, "Energy Efficient Adaptive Routing Algorithm in MANET with Sleep Mode", International Journal of Advanced Computer Research Volume-2, Number-4, Issue-6, December-2012.

[17] Dr. Sanjay Sharma, Pushpinder Singh Patheja, "Improving AODV Routing Protocol with Priority and Power Efficiency in Mobile Ad hoc WiMAX Network", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 1.