IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 42-45
www.iosrjournals.org

Managing the Threat of Denial of Service Attacks in MANETs

Prof. Deepali O. Bhende
Department of Computer Application, Ramdeobaba College of Engineering and Management, Nagpur, India

ABSTRACT : *A Mobile Ad-hoc Network (MANET) is an independent and self-configurable network without any fixed infrastructure. Compared to traditional network, MANETs have unique characteristics such as wireless shared radio medium, limited communication range, highly dynamic topology, power constraints and lack of trusted centralized authority. In addition to ensuring confidentiality and fidelity of acquired data, there is a demand for smooth transmission of information throughout the network. This requires unscathed service and continuous availability of network resources for the full duration of the network's operation. In contrast to this crucial objective of MANET management, a Denial of Service (DoS) attack targets to jeopardize the efficient use of network resources and disrupts the essential services in the network. Because of the wide range of methods used for creating a denial of service situation in the network, DoS attack could be considered as one of the major threats against MANET security. This paper aims to classify DOS attacks on MANETs, which are primarily performed on network and lower layers. Counter measuring techniques of these DOS attacks are also presented.*

Keywords *– MANET attack, DoS attack*

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system that consists of a variety of mobile hosts forming temporary network without any fixed infrastructure. Since it is difficult to dedicate routers and other infrastructure in such network, all the nodes are self-organized and collaborated to each other. All the nodes as well as the routers can move about freely and thus the network topology is highly dynamic. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments. There are 15 major issues and sub issues involving in MANET [10] such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. The routing protocol sets an upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. The problem is enlarged by the fact that routing usually needs to rely on the trustworthiness of all the nodes that are participating in the routing process. It is hard to distinguish compromised nodes from nodes that are suffering from bad links. The main objective of this paper is to discuss different DoS attack and their countermeasures with respect to network layer.

II. DOS ATTACKS IN MANETS

The MANETs are susceptible to many security issues. Characteristics as dynamic topology, resource constraint, limited physical security and no centralized infrastructure make those networks vulnerable to passive and active attacks. In passive attacks, packets containing secret information might be eavesdropped, violating the confidentiality principle. Active attacks include injecting packets to invalid destinations, deleting packets, modifying contents of packets, and impersonating other nodes.

Classifying attacks by network protocol stack is the more frequent. Table 1summarizes the main attacks for MANETs according to network layers. Some attacks are also categorized as byzantine or misbehavior attacks, being generated by network node whose actions cannot be trusted or do not conform to protocol specifications. Black hole, wormhole, rushing, Sybil, sinkhole, HELLO flooding and selective forwarding are examples of byzantine attacks. Moreover, these attacks are also related to selfishness problem. The goal of a selfish node is to make use of the benefits of

participating in the ad hoc network without having to expend its own resources in exchange .Researches have actively exploring many mechanisms for securing mobile ad hoc networks. These mechanisms are based essentially on customized cryptographic primitives, protocols for path diversity, protocols that overhear neighbor communication, and protocols that use specialized hardware.

Table 1: Summary of DoS attacks

Layer	**Attack**	**Description**
Physical	Jamming	deliberates interference with radio reception to deny the target's use of a communication channel
Link	Exhaustion	attacker induces repeated retransmission attempts in order to exhaust target's resources
	Collision	deliberates collisions or corruption induced by an attacker in order to deny the use of a link
Network	Wormhole	adversaries cooperate to provide a lowlatency side channel for communication by means of a second radio with higher-power and long-range link
	Blackhole	adversaries advertise zero-cost routes to every other node, forming routing black holes
	Sinkhole	an attempt is made to lure traffic from the network to pass through an adversary in order to facilitate other attacks
	Flooding	overwhelms victim's limited resources: memory, processing or bandwidth
	Selective forward	malicious nodes behave like normal nodes in most time but selectively drop sensitive packets for the application. Such selective dropping is hard to detect
	Sybil	multiple fake identities will be created for adversary nodes, meaning that an attacker can appear to be in multiple places at the same time
	Rushing	adversaries quickly forward their route request (RREQ) messages when a route discovery is initiated, in order to participate any route discovery. This attack can be carried out against on-demand routing protocols, as AODV, DSR and others
Transport	SYN Flooding	classic TCP SYN flood where an adversary sends many connection establishment requests to a target node, overwhelming its resources

III. DEFENSE AGAINST DOS ATTACKS

As it is a known fact, cryptography is one of the most common and reliable means to ensure security in MANETS. The main notions for cryptography are confidentiality, integrity, authentication and non-repudiation. The cryptography is discussed in detailed in [5]. MANETS have certain challenges in key management due to lack of infrastructure, absence of dedicated routers and mobility of nodes, limited processing power and limitation of battery power, bandwidth and memory. The main

requirement to ensure security in MANETS is to have a secure routing protocol which should have properties to detect malicious nodes, guarantee of exact route discovery process, maintaining confidential network topological information and to be self-stable against attacks. SAR (Secure-Aware Ad Hoc Routing protocol), which defines a level of trust as a metric for routing and as an attribute for security for routing. SAR using AODV uses encryption and decryption process using a common key [6]. The main drawback with SAR protocol is whenever the levels of security rise; it needs different keys for different levels, thereby increasing the number of keys [4]. SEAD (Secure Efficient Ad Hoc Distance Vector Routing protocol) is mainly designed for DSDV (Destination-Sequenced Distance Vector). This protocol can overcome DoS, all types of routing attacks and resource consumption attacks. It uses one-way hash function without the usage of asymmetric cryptographic mechanism. The mechanism uses authentication to differentiate between malicious and non-malicious nodes, which in turn reduces resource consumption attacks launched by malicious nodes. SEAD avoids routing loops, but the drawback lies whenever the attacker uses the same metric and sequence number used for authentication were same by the recent update message and updates with new update message [7]. The research update message from this mechanism is that it can also be used for other distance vector routing protocols.

ARAN (Authenticated Routing for Ad Hoc Networks) is a security protocol based on cryptographic certificates which overcomes all types of attacks in the network layer. Three major properties of cryptography, authentication, integrity and non repudiation are supported with both DSR (Dynamic Source Routing) and AODV protocols [8] . Even though this protocol mechanism is quite robust against attacks, it is mainly based on prior security coordination among nodes which cannot be correctly assured always. The issue of a false certificate to a node violates the non-repudiation and authentication property directly. CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks is mainly used for selfishness detection in the MANETS through node co operation mechanism [9]. CONFIDENT Protocol: Cooperation Of Nodes -Fairness In Distributed Ad hoc Networks provides trust based routing security in MANETS [10]. Timed efficient stream loss tolerant authentication (TESLA) protocol proposes a security mechanism to avoid attacks in MANETS [11]. Some approaches that detect malicious behavior in the data forwarding phase are, WATCHERS (Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security) [12] is a protocol designed to detect disruptive routers in fixed networks through analysis of the number of packets entering and exiting a router. In this approach each router executes the WATCHERS protocol at regular intervals in order to identify neighboring routers that misroute traffic and avoid them [14]. SCAN (self-organized network layer security in mobile ad hoc networks) [12] focuses on securing packet delivery. It uses AODV, but argues that the same ideas are applicable to other routing protocols. SCAN assumes a network with sufficient node density that nodes can overhear packets being received by a neighbor, in addition to packets being sent by the neighbor. SCAN nodes monitor their neighbors by listening to packets that are forwarded to them. The SCAN node maintains a copy of the neighbor's routing table and determines the next-hop node to which the neighbor should forward the packet; if the packet is not overheard as being forwarded, it is considered to have been dropped [14]. Off late a system that can mitigate the effects of packet dropping has been proposed. This is composed of two mechanisms that are kept in all network nodes: a watchdog and a pathrater. The watchdog mechanism identifies any misbehaving nodes by promiscuously listening to the next node in the packet's path. If such a node drops more than a predefined threshold of packets the source of the communication is notified. The path rate mechanism keeps a rate for every other node in the network it knows about. A node's rate is decreased each time a notification of its misbehavior is received. Then, nodes' rates are used to determine the most reliable path towards a destination, thus reducing the chance of finding a misbehaving node along the selected path. Moreover, the watchdog might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions or nodes capable of controlling their transmission power. Such weaknesses are the result of using promiscuous listening to determine whether a node has forwarded a packet or not [13].

IV. CONCLUSION

Many complicated key exchange or distribution protocols have been designed, but for MANET, they are restricted by a node's available resources, dynamic network topology, and limited bandwidth. Efficient key agreement and distribution in MANET is an ongoing research area. Most of the current work is on preventive methods with intrusion detection as the second line of defense. One interesting research issue is to build a mechanism which uses many approaches together without the use of key management to ensure more level of security in MANET. Building a sound robust semantic security approach and integrating it into the current preventive methods can be done in future research. Since most attacks are unpredictable, a resiliency oriented security solution will be more useful, which depends on a multi-fence security solution.

REFERENCE

[1] C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Adhoc Networks. 19th *International Conference on Advanced Information Networking and Applications*, 2005. AINA 2010**,** Volume: 1, 72- 77 vol.1.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. *Security in wireless mobile ad hoc and sensor networks*, October 2007, page, 85-91

[3] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[4] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", *Low Price Edition, Pearson Education*, 2007, pp. 521.

[5] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996 .

[6] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks", *Proceedings of ACM MOBIHOC* 2001, pp. 299-302, October, 2001.

[7] Y.C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. *4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, June 2002, pp. 3-13.

[8] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks", *In Proceedings of the 10th IEEE International Conference on Network Protocols* (ICNP' 02), pp. 78-87, November 2002.

[9] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks*", IFIP-Communication and Multimedia Security Conference* 2002.

[10] S. Buchegger and J. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks", *Proc. of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands*, Spain, 2002.

[11] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol", Internet Draft, 2000.

[12] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Selforganized network-layer security in mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, February 2006, pp. 261- 273 systems for signal processing, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978.

[13] M. Patel, S. Sharma "Detection of malicious attack in MANET a behavioral approach" *3rd International Advance Computing Conference (IACC), IEEE* , Page(s): 388 – 393, 2013.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", in Proc. 6th ACM *International Conference on Mobile Computing and Networking*, , Boston, USA, August 2000, pp. 255-265.

[15] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", *Journal of Internet Engineering*, 2:1, 2008.