Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

DoS Attacks and Mitigation Techniques in Manet: A Review

Sakshi Gautam*, Suveg Moudgil
Computer Science and Engineering, Kurukshetra University,
Haryana, India

Abstract— The insecurity of the wireless links, energy constraints, insecure operational environment, lack of central authority and the vulnerability of statically configured security schemes are definitely such challenges. Each node in a MANET is capable of acting as a router. In this paper, we will present survey of common Denial-of-Service (DoS) attacks namely Wormhole attack, Flooding attack, Black hole attack and Gray hole attack which are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

Keywords— DoS attack, IDS, MANET, Mitigation, Security

I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. The recent advancements in the wireless technology and their wide-spread utilization have made tremendous enhancements in productivity in the corporate and industrial sectors. Wireless networks find applications in several areas such as military applications, natural calamities such as earthquakes, and rescue activities. In the past few decades, security in the military operations is exposed to vulnerabilities like eavesdropping and modifying the data causing havoc in military camps. Consequently military applications required quick and reliable communication to exchange the data and stay away from enemy intrusion. Since the wireless shared medium is completely exposed to outsiders, it is susceptible to attacks that could target any of the OSI layers in the network stack. For example, jamming of the physical layer, disruption of the medium access control (MAC) layer coordination packets, attacks against the routing infrastructure, targeted attacks on the transport protocol, or even attacks intended to disrupt specific applications. Recent trends in military operations require the communication to enforce requirements like reliability, efficiency, secure communication, and support for multicast routing. However, in MANET mobile entities are prone to various security attacks due to dynamic changing topology, shared and error-prone channel, open medium and inhibited by limited availability of resources such as bandwidth, battery, and computational power. Due to unique characteristics of wireless networks the effects of applying the security techniques used in wired networks, such as access control and authentication, to wireless and mobile networks.

II. DOS ATTACKS IN MANET

DoS attack is an attempt to make resources or services unavailable to their intended users. It is a severe threat for MANETs because they can be crashed due to their limited battery power or their network can easily become congested due to its relatively limited bandwidth compared to fixed networks. Common DoS attacks are:

- Wormhole attack: It lures traffic through a very long path by giving false information to the nodes about the distance between them.
- Black hole attack: It is also known as packet drop attack. A router that is supposed to relay packets instead discards them.
- Gray hole attack: It is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source node.
- Flooding attack: It is a DoS attack in which the malicious node broadcast the redundant false packets in the network to exhaust the available resources and reduces the throughput of the network so that valid users are not able to use the network resources.

III. MITIGATION TECHNIQUES AGAINST DOS ATTACK

A variety of security techniques have been proposed in the literature against DoS attacks. The conventional techniques such as symmetric cryptography, asymmetric cryptography and identity based cryptography serve as first line of defense. Second line of defense such as, Intrusion Detection Systems (IDS) has been used to detect anomalies in MANET.

A. Prevention Techniques

Yil et al. [3] analysed the flooding attack on the entire network performance under the circumstances of different flooding frequency and different number of attack nodes. To reduce congestion in a network, the existing protocol (DSR, AODV, DSDV and others) adopts various constraints. But the attacker node violates the constraints to exhaust the network resources.

The authors showed that, with the increase of flooding frequency and the number of attack nodes, network performance drops. In addition, with the increasing frequency of flooding attacks, the packet delay firstly increases and then declines to a value of stability in the end.

Xing et al. [4] proposed a semi-Markov process model to characterize the evolution of node behaviours and investigated the problem of node isolation where the effects of DoS attacks are considered. In this (i) semi-Markov process (SMP) is used to characterize the evolution of node behaviours (ii) node isolation problem is revisited by examining the cooperative degree and (iii) survivability of wireless ad hoc networks is analysed probabilistically, which is used to quantify the impacts of different behaviours.

Kim et al. [5] proposed a period based defense mechanism against data flooding attacks. The current defense systems focus on RREQ flooding attacks rather than the data flooding attack. They easily reduce the throughput of burst traffic by comparing with the simple threshold. The proposed scheme uses a blacklist, considers the data type, and processes packets according to the priority so as to defend against data flooding attacks; since the attacker forwards many data packets at a high rate for the whole session. The proposed scheme is useful to networks where burst traffics are transferred because many users tend to download and share multimedia data.

Albandari et al. [6] proposed an enhanced Ant based Defense Mechanism for Selective Forwarding Attack in MANET. First, we have implemented S-ACK scheme to transmit the secure acknowledgement. To detect attackers, a trust model is designed. The Forward ant agents transmit back the digitally signed S-ACK through the Backward Ant agent to detect any selective forwarding attack against any source node. Also a Challenge and Monitoring packet is transmitted by source node to monitor the neighbour node and the verification table updated by an ant agent.

Singh et al. [7] proposed Mitigation of DoS Attacks by using multiple encryptions in MANETs. They used hybrid security approach based on AES (Advance Encryption Standard) with Blowfish Algorithm.

B. Detection Techniques

Prevention based techniques such as authentication and encryption are not good solution for ad hoc networks to eliminate security threats because prevention based techniques cannot protect against mobile nodes which contain the private keys. So the Intrusion detection system is an essential part of security for MANETs. It is very effective for detecting the intrusions and usually used to complement for other security mechanism. That's why Intrusion detection system (IDS) is known as the second wall of defense for any survivable network security [1].

When any set of actions attempt to compromise with the security attributes such as confidentiality, repudiation, availability and integrity of resources then these actions are said to be the intrusions and detection of such intrusions is known as intrusion detection system (IDS) [2]. The basic functionality of IDS depends only on three main modules such as data collection, detection and response modules. The data collection module is responsible for collecting data from various data sources such as system audit data, network traffic data, etc. Detection module is responsible for analysis of collected data. While detecting intrusions if detection module detects any suspicious activity in the network then it initiates response by the response module.

There are many numbers of IDSs that have been proposed in MANETs. Sujatha et al. [8] proposed a new fuzzy based response model (FBRM) for analysing the internal attacks in mobile ad hoc network. They have considered false route request (FRR) attack that causes flooding, congestion, DoS attack, exhaustion of resources and exhaustion of bandwidth at nodes in the MANETs. The FFR attack can be detected by monitoring various features such as route request rate, sequence number, Acknowledgement time and load pattern.

Andrea and Hooman [9] suggested artificial immune system for detecting misbehaving nodes in Ad-Hoc wireless networks which is based on type-2 Fuzzy set. The purpose of this work is to detect and learn about misbehaving nodes as well as protect the network without human interference.

In [10], the author proposed trust estimation technique which uses the DSR on demand routing protocol to detect & mitigate the effect of RREQ flooding attack in the networks with high node mobility. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they define the threshold values.

Kulbhushan et al. [11] proposed a fuzzy logic based IDS which can detect black hole attack on MANETs. They formed the rule for detecting attack based on Mamdani fuzzy model and for drawing the membership function, input parameters such as forward packet ratio and average destination sequence number selected in each time slot. The output of derived rule is dependent on the fidelity level of each node. If calculated fidelity level of node is less than or equal to fidelity threshold value then node is black hole otherwise node is not black hole. Ultimately fidelity level shows the level of node.

M. Wahengbam et al. [12] suggested a fuzzy based IDS for MANETs which is capable to detect packet dropping attack such as Black hole and Gray hole attack. They considered that each node is having IDS and detect malicious activity locally for this purpose and assumed some threshold value for each node. In this proposed approach, each node maintains its packet list with the feature: sequence no., source node, destination node, packet type and expire time.

Manoj V. et al. [13] presented a scheme based on certification authority (CA) and fuzzy logic for MANETs. Some central node is authorized by service provider for assigning the keys to source node which is going to request in the network called certification authority nodes and with the help of trust agent, direct and recommended trust values are obtained periodically. A proposed fuzzy logic based analyzer is used to calculate the trust value of a requested node (which is ready to data exchange between source and destination in the network) based on the computed fuzzy table. If requested node is trusted then it would get the certification otherwise not.

Vydeki et al. [14] used Fuzzy interference system for detection of Black hole attack They advised that selection of clustering algorithm in the process of FIS based IDSs plays an important role so it compared two well known clustering approaches such as subtractive and Fuzzy c-mean clustering. This proved that the detection rate based subtractive clustering (97%) is more efficient than the fuzzy c-means clustering (91%).

Shamshirband et al. [15] proposed a bio-inspired method, namely the cooperative-based fuzzy artificial immune system (Co-FAIS). It is a modular-based defense strategy constructed as multi-agent, providing defense against a single attacker. It detects danger signals (based on antigen or attack patterns) emitted by sensor nodes. In such a multi-node circumstance, the sniffer module adapts to the sink node to audit data by examining every packet constituent and sending the log file to the next layer.

E. Vishnu Balan et al. [16] proposed a system to detect the malicious behaviour of node by intrusion detection system with fuzzy logic technique. The system is robust enough to detect attacks such as black hole attack and gray hole attack and uses efficient blocking mechanism to prevent the attacks and provides a secure communication between nodes. This method not only identifies the attack, but also identifies the range and extension of attack.

K.S. Sujatha et al. [17] proposed a technique to analyse the exposure to black hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system analyses the behaviour of every node and provides details about the attack. The performance of MANET is analysed based on Genetic Algorithm Control (GAC). GAC is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on.

Table I Comparison of mitigation techniques against DoS attack in MANET

Authors	Technique	Detection/ Prevention Scheme	Merits	Attacks
S.Sujatha et al., 2008	Fuzzy logic controller based intrusion handling system	IDS(Fuzzy based response model)	Identifies the attack and detect the level of intrusion and takes appropriate steps to make the system immune	False route request attack (FRR)
Andrea and Hooman, 2010	A Biologically – Inspired type-2 fuzzy set based algorithm	IDS(Type-2 Fuzzy set)	Minimize the uncertainties in the network	Misbehaving Nodes
Kim et al., 2010	Novel Defense Mechanism against Data Flooding Attacks	Prevention (Defense mechanism)	Useful to networks where burst traffics are transferred	RREQ flooding attacks
Shishir K. Shandilya et al., 2010	A Trust Based Security Scheme for RREQ Flooding Attack in MANET	IDS(Trust Estimation)	Concept of delay queue reduces the probability of accidental blacklisting of the node	RREQ flooding attack
Kulbhushan et al., 2011	Fuzzy Logic Based Intrusion Detection System	IDS(Mamdani Fuzzy model)	Improves the performance of AODV	Black hole
Manoj V. et al., 2012	A Novel security framework using trust and fuzzy logic in manet	IDS(Trust and Fuzzy logic based)	Only trusted nodes get the certification	Malicious node
M.Wahengbam et al., 2012	Intrusion detection using fuzzy logic	IDS(Fuzzy)	Degree of maliciousness of a node can be identified	Black hole, Gray hole
Vydeki et al., 2013	Fuzzy based hybrid intrusion detection system	IDS(FIS-Fuzzy Interference System based)	Specification and anomaly based detection from Data packets and Control packet based features	Black hole attack
Shamshirband et al., 2014	Co-FAIS (Cooperative Fuzzy Artificial Immune System	IDS (Fuzzy Q-learning based)	Efficient in terms of detection accuracy, network lifetime and	DDoS attack

	for Detecting Intrusion in Wireless Sensor Networks)		energy consumption.	
Albandari et al., 2015	MrDR Method to detect DoS Attacks in MANET	Prevention(MrDR-Monitoring, Detection, and Rehabiliation)	Increases network performance considerably	DoS Attack
Singh et al., 2015	Multiple encryptions in MANETs	Prevention(AES-Advance Encryption Standard and Blowfish algorithm)	Hybrid security approach	DoS Attack
K.S. Sujatha et al., 2012	Design of Genetic Algorithm based IDS for MANET	IDS (GA-Genetic Algorithm)	Detect vulnerabilities in AODV	Black hole
E. Vishnu Balan et al., 2015	Intrusion detection system with fuzzy logic technique	IDS (Fuzzy)	Secure data communication over the network	Black hole, Gray hole

IV. CONCLUSIONS

The security issues have been ignored while designing of most of the MANET routing protocols. This paper provides brief overview about security issues for MANET. DoS attacks breach network's security and disrupt network operations. We described various DoS attacks like Wormhole, Black hole, Flooding and Gray hole attacks and surveyed few existing solutions for defense against these attacks. Extensive research is required for efficient discovery and prevention of these DoS attacks.

ACKNOWLEDGMENT

I would first like to thank my guide Er. Suveg Moudgil, Associate Professor of the Department Of Computer Science and Engineering, Kurukshetra University. His consistent support and intellectual guidance steered me in the right direction whenever I had a question about my research or writing.

I would also like to acknowledge Er. Navdeep Kumar, H.O.D of the Department Of Computer Science and Engineering, Kurukshetra University as the second reader of this review paper, and I am gratefully indebted to him for his very valuable comments on this work.

REFERENCES

[1] Y. Zhang and W. Lee., *Intrusion detection in wireless ad hoc networks*, In Proceedings of the 6th Annual *Interntional Conference on Mobile Computing and Networking(MobiCom'00)*, pages 275-283, 2000.

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla, The architecture of a network level intrusion detection system Technical report, Computer Science Department, University of New Mexico, August 1990.

[3] Yil P, Wu Y and Ma J, Experimental Evaluation of flooding attacks in mobile ad hoc networks, Proceedings of *IEEE International Conference on Communications*, pp. 1-4, 2009.

[4] Kim H, Bhargav Chitti R and Song J, Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks, *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 579-582, 2010.

[5] Xing F and Wang W, On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures, *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, 2010.

[6] Alsumayt, Albandari; Haggerty, John; Lotfi, Ahmad, Performance, Analysis, and Comparison of MrDR Method to detect DoS Attacks in MANET, in *Intelligence and Security Informatics Conference (EISIC)*, 2015 European , pp.121-124, 7-9 Sept. 2015.

[7] Singh, A.V.; Chattopadhyaya, M., Mitigation of DoS at tacks by using multiple encryptions in MANETs, in Reliability, *Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)*, 2015 4th International Conference on , vol., no., pp.1-6, 2-4 Sept. 2015.

[8] S. Sujatha, P. Vivekanandan, A. Kannan, Fuzzy logic controller based intrusion handling system for mobile ad hoc networks, *Asian Journal of Information Technology*, pp.175-182, 2008.

[9] A. Visconti, H. Tahayori, A Biologically – Inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad hoc networks, *International Journal for Infonomics*, Vol.3, No.2, pp. 270-277, June 2010.

[10] Shishir K. Shandilya, Sunita Sahu; A Trust Based Security Scheme for RREQ Flooding Attack in MANET; *International Journal of Computer Applications* (0975 – 8887) Volume 5– No.12, August 2010, pp 4-8.

[11] Kulbhushan and J. Singh, Fuzzy logic based intrusion detection system against blackhole attack AODV in manet, *IJCA Special issue on "Network Security and Cryptography"* Vol. NSC, No. 2 pp. 28-35, December, 2011.

[12] M. Wahengbam and N. Marchang, Intrusion detection in manet using fuzzy logic, 3rd *IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS)*, pp. 189 – 192, Shillong, 30-31 March 2012.

[13] V. Manoj, M. Aaqib, N. Raghavendiran and R. Vijayan, A Novel security framework using trust and fuzzy logic in manet , *International Journal of Distributed and Parallel Systems* , Vol. 3, No. 1, pp. 285-298, January, 2012.

[14] D. Vydeki and R.S. Bhuvaneswaran, Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks, *Journal of Computer Science*,Vol. 9, No. 4, pp. 521-525, 2013.

[15] Shamshirband et al., Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. *Journal of Network and Computer Applications* 42 (2014), pp. 102-117.

[16] E. Vishnu Balan, M.K. Priyan, C. Gokulnath, and G. Usha Devi, Fuzzy Based Intrusion Detection Systems in MANET, *Procedia Computer Science*, vol. 50, pp.109-114, 2015.

[17] K. S. Sujatha and R. S Bhuvaneshwaran, *Design* of genetic algorithm based IDS for MANET, in Proc. th*e IEEE Conference ICRTIT*, 2012.

