Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Review on the Flooding Attacks in Mobile Ad Hoc Networks

**Jasmeen Mangat**
M.tech (cse ) & Guru Kashi University,
Talwandi Sabo, Bathinda,
Punjab, India

**Er. Jaspreet Kaur**
Assistant Professor & Head
Guru Kashi University, Talwandi Sabo
Bhatinda, Punjab, India

***Abstract:*** ***The present times witness the rise of the wireless communication between almost every pair of the devices present around us. The Mobile ad hoc networks (MANETs) is one of the greatest innovations of the mankind which enables two users to communicate over vast distances. The multi hop nature of the message transmission brings along with it the serious security concerns. The devices need to work longer for the complex applications and other uses. The attacks focused at draining or consuming of the batteries such as flooding attack becomes important to study in the view of energy conservation and enhancement of the network lifespan. This paper shows the various studies regarding the DDoS Flooding attack in the networks.***

***Keywords: MANETs, DDoS, Flooding, network lifespan.***

## I. INTRODUCTION

In recent decades, there has been a tremendous measure of investigation concerning wireless sensor systems routing and the field of remote and mobile systems has experienced a broad development. This has come about into the improvement of minimal effort, low-force, multi-purpose little sensor nodes. Mobile Ad Hoc Networks (MANETs) has turned into a standout amongst the most common zones of examination as it postures different difficulties to the security of the packets exchanged during the communication.

In this technological era, communications technology has been continuously evolving at an enormous pace. Individuals can deploy a wireless network easily and quickly. End clients can move around while staying associated with the system. In an infrastructure network, nodes are obliged to be in the scope region of access point. In this way, mobility is limited with the distance between the access point and the node. However, in an Ad-hoc system, a node can transmit information to another as long as there is a third node that can mutually communicate with both of them. Data is forwarded via intermediate node/s using one of the ad-hoc network routing protocols. This methodology backs a bigger working region however physical layer complexity increases. Malicious nodes may scan for the destination node that is out of range by flooding the network with broadcasts that are forwarded by each node. In an ad-hoc network, power consumption is higher, since nodes transmit packets that do not concern themselves.

Owing to these characteristics of the mobile ad hoc networks, any attacker with an aim of disrupting the services of the network can hack a node or compromise the functioning of the normal node. The compromised node can be programmed to flood the networks for finding the path to destination not present in the network. This continual flooding of the packets thus cause harm to the batteries of the devices. This paper thus taking into consideration the adverse effects of the flooding attack, describes various approaches that deal with the identification and protection against such attacks. Section II therefore represents the previous studies with the conclusion being shown in the section III.

## II. LITERATURE REVIEW

1. The paper **B. B. Gupta, Student Member, IEEE**, **R. C. Joshi, and Manoj Misra** presents an overview of the DDoS problem, available DDoS attack tools, defense challenges and principles, and a classification of available DDoS prevention mechanisms. The study helps to provides better understanding of the problem and enables to develop a proper prevention mechanism for fighting against DDoS threat.
2. The paper **Kavuri Roshan, K.Reddi Prasad, Niraj Upadhayaya & A.Govardhan**, proposed the period-based defense mechanism against data flooding attacks. However, 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 paper aims to enhance the throughput of burst traffic under the data flooding attack. 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.
3. This paper **Minda Xiang, Yu Chen; Wei-Shinn Ku; Zhou Su** proposes a strategy to mitigate DDoS attacks in MANETs. The proposed strategy includes high redundancy and selection of protection node. Once a DDoS attack has been detected, the suspicious traffic will be redirected to the protection node. The victim will function normally, and it is reasonable to expect that the attacker will stop the meaningless efforts. The paper verified the effectiveness of the proposed approach and evaluated the cost and overhead of the system by intensive

 

simulation experiment using NS-2. The paper also evaluated the cost of the protocol, and the results are found encouraging. The overheads are small to implement the DDoS mitigating scheme on top of the well-known AODV protocol.

4. The proposed work **Vatsa Rupa Rani, A.K.** developed a CARD (continuous and random dropping) detection mechanism which reduces deficiency of the reduction of Quality (RoQ) to the mobile nodes. The proposed rate limiting scheme will penalize the different attackers based on their rate limits and server load. The victim end defense system decreases the rate limit exponentially and increase it linearly based on the attack traffic rate. Hence CARD based DRDOS attack detection and prevention techniques has been proposed for MANET for smooth and high data rate communication over MANET. When the total traffic load exceeds the threshold, an attack is detected. Finally, this approach is discussed in three phases as detection, control and prevention which is explained in CARD detection architecture.
5. This paper **Yogesh Chaba, Yudhvir Singh**, **Prabha Rani**, implemented two types of Passive DDoS based attack mechanisms- Packet Dropping Based Passive DDoS Attack and Selfish Node Based DDoS Attack. The impact of Packet Dropping and Selfish Node based Passive DDoS attack is evaluated by finding the packet delivery ratio, energy consumption and collisions by varying node mobility and number of attackers. Experiments are performed by implementing both types of attacks through simulation. It is found that selfish node based Passive DDoS attack have greater impact on network performance.
6. The paper **Ramratan Ahirwal,** describes that MANETs are vulnerable to Distributed Denial of Service (DDoS) due to their salient characteristics which shows there is an immediate need to provide an incentive mechanism that can provide cooperation among nodes in the network and improve overall network performance by reducing DoS attacks. The paper presents a new defense mechanism which consists of a flow monitoring table (FMT) of all the mobile node. The result analysis is done on the bases of actual TCP flow monitoring, routing load, packet delivery ratio and average end-to-end delay in normal, DDOS attack and IDS time.
7. The paper **Yu, Xuan** presents the security solution for AODV and AODV-like networks from a novel perspective. The proposed defense system is based on proxy-based overlay architecture. The proposed solution assures a minimum impact on the objective system infrastructure or the network communication interface to make it easy to implement and update, while providing an acceptable secure protection against DDoS attacks, such as Router Requirement (RREQ) flooding, data flooding and black-hole.
8. The paper **Yinghua Guo** displays a dispersed examining system to distinguish and moderate noxious packet dropping in remote specially appointed net- lives up to expectations. In the distributed testing strategy, each node in the system will test alternate nodes occasionally to locate if any of them neglect to perform the sending capacity. Accordingly, node state data can be used by the routing algorithm to sidestep those malicious nodes. The simulation trials are performed in Ns2.

Table: 1 The following table is based on the techniques used and operations and the fields on which the techniques are based.

| Technique Used | Operation | Focuses on |
|---|---|---|
| Period Based Defense Mechanism [2] | Checks data packet floods at the end of each period in order to enhance the throughput of burst traffic. | Improving the throughput of the network. |
| Protection Node based Strategy [3] | Defines the priority level for the nodes. Lower level nodes protect higher level nodes and Protection nodes are selected to supervise malicious flows, and meanwhile, to protect the victim nodes. | Reducing the delay and drop rate in the network. |
| CARD [4] | Makes use of rate limiting scheme to penalize the different attackers based on their rate limits and server load. | Smooth and high data rate communication over MANET. |
| FMT (Flow Monitoring Table) based IDS [6] | It checks the normal and abnormal behavior of the network according to threshold level. If information deviates more or less than 10 percentage then network is considered as infected. | Detection of the malicious node and data recovery. |
| Policy Based Preventive Measure [9] | Compares the number of request packets sent with number of neighbors to detect malicious node. | Improving Packet Delivery ratio and throughput. |

 

**9.** In this scheme **Mohan Kumar S B, Anand Vijay K M, Suhas N S,**the authors have put forward the scheme to detect and prevent flooding attacks. In this, when source wants to find a path to the intended destination node, it would forward the RREQ packets to its neighbors. The neighbors re-broadcast the same when route is not available with them. Normally, in the absence of any attacker, the node tends to broadcast the very less RRE packet to their neighbors. But attacker node would flood such packets. According to the existing scheme, if any node is found to broadcast number of packets more than the number of neighbors it possesses it would be suspected of being involved in unnecessary flooding of the packets. By keeping an eye on the packet forwarding behavior of the node and comparing it with the number of neighbors, the attacker would be detected easily.

## III. CONCLUSION

This paper shows the brief explanation of various schemes that have been formulated by the investigators in the older times to identify and prevent against malicious node causing the flooding of the packets in the network. The authors in [9] have successfully done the identification and prevention of the same attack. However, they have focused on another major problem where the malicious node can fake its ID and continue with the flooding process. So in the future, we would like to propose a scheme that takes into account the spoofed flooding attack so that network can have more security.

## REFERENCES

[1] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE, "Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163.

[2] Kavuri Roshan, K.Reddi Prasad, Niraj Upadhayaya & A.Govardhan, "New-fangled Method against Data Flooding Attacks in MANET", International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 3, June 2012.

[3] Minda Xiang, Yu Chen; Wei-Shinn Ku; Zhou Su, "Mitigating DDoS Attacks Using Protection Nodes in Mobile Ad Hoc Networks", Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE.

[4] Rupa Rani, A.K. Vatsa, "CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET", International Journal of Engineering and Technology Volume 2 No. 8, August, 2012.

[5] Yogesh Chaba, Yudhvir Singh, Prabha Rani, "Comparison of Various Passive Distributed Denial of Service Attack in Mobile Ad hoc Networks", ISSN: 1790-5117, ISBN: 978-960-474-155-7, Recent Advances in Electronics, Hardware, Wireless and Optical Communications.

[6] Ramratan Ahirwal, "Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network", International Journal on Computer Science and Engineering (IJCSE)

[7] Yu, Xuan, " A Defense System On DDos Attacks in Mobile Ad Hoc Networks".

[8] Yinghua Guo, "Defending MANETS against Flooding Attacks by Detective Measures".

[9] Mohan Kumar S B, Anand Vijay K M, Suhas N S, "A Policy based preventive measure against flooding attack in MANETs", IEEE International Conference on Recent Trends in Electronics Information Communication Technology, May 20-21, 2016, India.

 