

## **Security Mechanism for Mitigation of Flooding Attack under Group Mobility Model in MANET**

**Kashif Kawsar Qadri and Vishali Sharma**

*<sup>1</sup>Student, <sup>2</sup>Faculty, Lovely Professional University*

### **Abstract**

Mobile Ad-hoc network (MANET) is collection of infrastructure less, decentralized self-directed nodes which form the dynamically a temporary network for transmitting data. These nodes are basically the systems or devices which can act simultaneously as host and router. These nodes have self alignment ability thus can be positioned instantly without any need of infrastructure. Because of the dynamic nature of the MANETs they are more prone to the attacks. Out of these attacks flooding attack is one of them. There are many routing protocols which have been developed for the MANETs out of these protocols Ad hoc on demand distance vector protocol (AODV) is one of them. In this paper the detection of flooding attack on the AODV protocol is being presented using group mobility model. This is the simulation based study in which throughput, Packet delivery ratio (PDR), and overhead has been simulated and studied. It was observed that the value of throughput and PDR increased up to 73. 20 and 0. 9948 respectively while as the value of overhead decreased to 1. 4139. The simulation tool used for the study was NS-2. 5.

**Index Terms-** MANET, Flooding Attack, AODV, PDR, Overhead.

### **I. INTRODUCTION**

MANET is a self-configuring infrastructure less network of mobile devices also called nodes which are connected by wireless medium. These nodes are basically the systems or the devices which can simultaneously act as host as well as router. These nodes have the self configuration ability thus can be immediately positioned without any need of the infrastructure. Due to the features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense the security remains main concern in MANETs [1].

At present, several effective routing protocols have been projected. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol. AODV [2] is a reactive routing protocol designed for a mobile ad hoc network. In AODV, when a source node desires to propel a data packet to a destination node and does not have a route to destination node, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node [2]. While as in proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol nodes find routes by periodic exchange of topology information.

MANETs have the dynamic nature due to this they are more prone to the attacks. Out of these attacks the flooding attack is one of them. Ad Hoc Flooding Attack is a consequence in denial of service when used against all previously on-demand ad hoc networks routing protocols. In this attack, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks so as to congest in links [3]. The aim of the flooding attack [4] is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

## **II. RELEATED WORK**

In this section, some of these contributions related to the flooding attack in MANETs is been presented.

Taranpreet Kaur et. al [5] presented a new approach which efficiently defends from RREQ Flooding attack in military battlefield situations. They observed that if all malicious nodes are present in one cluster the performance degradation is more, as clustering overhead increases. Ping Yi et. al [6] presented a New Routing Attack in Mobile Ad Hoc Networks by using the method of neighbor suppression is which each neighbor calculates the rate of RREQ originated by intruder. They observed that If the rate exceeds some threshold, all neighbors will not receive and forward packets from intruder. Meghna Chhabra et. al [7] proposed the solution to Handle DDOS Attack in MANET. They observed that if the monitored node and will wait for its reply. If it does not get reply within the set interval then the node being monitored is flooded

node that is the victim node.

Alokparna Bandyopadhyay et. al [8] proposed a Simulation Analysis of Flooding Attack in MANET by identifying the impact of flooding attack on it. They observed that the presence of malicious flooding nodes in MANET can affect the performance of the overall wireless network and can act as one of the major security threats and due to the extensive flooding in the network, average percentage of packet loss, average routing overhead and average bandwidth requirement– all increases, thus decreasing the overall network throughput.

### **III. AODV AND ITS SECURITY THREATS**

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In AODV, the network is silent until a connection is necessary. At that point the network node that needs a connection broadcasts a demand for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of limited routes back to the needy node. When a node receives such a message and by this time has a route to the desired node, it sends a message in reverse through a temporary route to the requesting node. The needy node then begins using the route that has the minimum number of hops through other nodes. Vacant entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process reruns. Much of the complication of the protocol is to the minimum number of messages to conserve the space of the network. Such as, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have previously passed on. One more feature is that the route requests have a "time to live" number that limits how many times they can be readdressed. Another such feature is that if a route request fails, one more route request may not be sent until twice as much time has taken place as the timeout of the previous route request.

The advantages of the using AODV protocol is that it creates no extra traffic for communication along existing links and makes distance vector routing so simple, and doesn't need much memory or calculation with less connection setup delay while as it has also a disadvantage of intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a greater but not the latest destination sequence number, thereby having stale entries.

Some of the security attacks that threatens the AODV are as:

#### **A. *Attacks using Alteration***

Alteration is a type of attack when an authorized party not only boosts access to but tinkers with an asset. For example a malicious node can redirect the network traffic and plan DOS attacks by modifying message fields or by forwarding routing message with distorted values.

**B. Attacks using Masquerade**

As there is no authentication of data packets in modern ad-hoc network, a malicious node can fire many attacks in a network by masquerading as another node i. e. spoofing. Spoofing occurs when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and changes the target of the network topology that a benign node can either.

**C. Attacks through Fabrication**

Fabrication is an attack in which an authorized party not only achieves the access but also embeds counterfeit objects into the system. In MANET, fabrication is used to indicate the attacks performed by generating distorted routing messages.

**D. Grayhole Attack**

The grayhole attack has two different phases. In the first phase, a malicious node manoeuvres the AODV protocol to advertise itself as having a credible route to a destination node, with the motive of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a positive probability. This attack is more severe to detect than the blackhole attack where the malicious node drops the received data packets with certainty. A gray hole may display its malicious behaviour in alternate ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while progressing all the packets for other nodes. Other type of grayhole node may behave maliciously for some duration by dropping packets but may switch to normal behaviour in the near future. A gray hole may also display a behaviour which is a combination of the above two, thereby making its detection even more troublesome.

**E. Wormhole Attacks**

Wormhole attack is also known as *tunnelling attack*. A tunnelling attack is where two or more nodes may cooperate to encapsulate and exchange messages between them along the previous data routes. This exploit gives the chance to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is guarded by the two colluding attackers.

**F. Lack of Cooperation**

Mobile ad-hoc networks depend on the combination of all the participating nodes. The maximum number of nodes cooperates to transfer traffic, the more powerful a MANET gets. But one of the distinct kinds of misbehaviour a node may show is selfishness. A selfishness node wants to preserve own resources while using the services of others and captivating their resources.

**IV. RESEARCH METHODOLOGY**

In this proposed work following are the methods which were being implemented:

### **A. Neighbour Selection**

Source node selects its neighbour nodes within the range of 250 meters then divides nodes which comes within 200 meters where cluster of nodes is formed and nodes which come within 50 meters of range. Nodes present in the range of 200 meters broadcasts route request packet to nodes which come within the range 50 meters, these nodes are considered to be monitoring nodes. These monitoring nodes will check the RREQ\_Broadcast rate for every selected nodes which comes within 200 meters of range from source node.

### **B. Updating Routing Table**

Monitoring node will send route reply packets back to the source node about the collecting information from selected node which are with in the range of 200 meters from source node. Then source node will check its routing table entries if RREQ\_Broadcast rate of selected nodes rate is greater than RREQ accept limit rate, then node is considered to be a malicious else if RREQ\_Broadcast rate of selected node is smaller than RREQ accept limit rate then node is considered to be genuine node.

### **C. CLUSTER HEAD FORMATION**

After source node making changes in routing table entries will select a genuine node which will be closer to destination node is selected as cluster head and malicious node will be isolated from other intermediate node. In similar way other cluster of nodes will be formed with their respective cluster heads which will be close to destination, after which data is send from source to destination via different intermediate cluster heads.

## **V. SIMULATION WORK**

The metrics in the Network Simulation are the chief aspects of network performance, which have been used to associate the performance of the anticipated scheme in the network with the performance of the actual protocol.

### **A. Throughput**

It is the rate of successful message delivery past a communication channel. This data may be sent over a physical or logical link, or pass through a sure network node. The throughput is constantly measured in bits per second (bit/s or bps), and occasionally in data packets per second or data packets per time slot. The system throughput or aggregate throughput is the sum of the data rates that are delivered to every terminal in a network. Throughput is necessarily synonymous to digital bandwidth consumption. It is sum of sizes (bits) or number (packets) of generated/sent/forwarded/received packets calculated at every time interval and divided by its length. Throughput (bits) is shown in bits. Throughput (packets) shows numbers of packets in every time interval. Time interval length is equal to one second by default.

### B. Packet Delivery Fraction (PDF)

Packet Delivery Fraction (PDF): This is calculated as the ratio of total number of packets received by the destination nodes to the number of packets sent by the source nodes. It is the ratio of number of delivered data packets to the destination. This illustrates the level of delivered data to the destination.

$$\frac{\sum \text{Number of packets received}}{\sum \text{Number of packets sent}}$$

### C. Overhead Time

It is defined as time taken for processing of data, routing execution, and command execution.

Following is the table which describes the NS-2. 5 simulation setup for wireless networks.

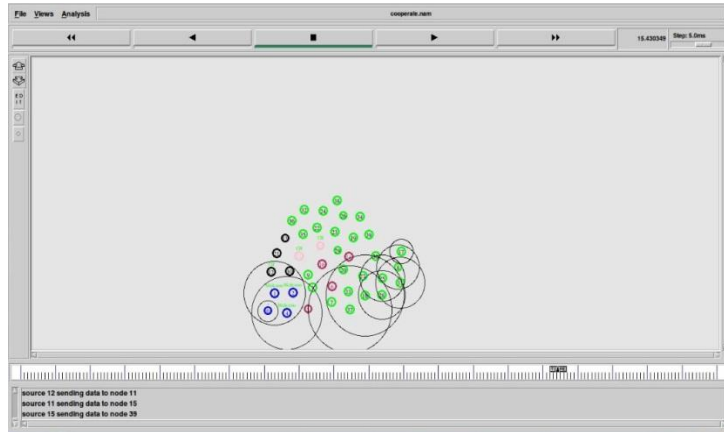
**Table 1: NS-2. 5 Simulation Setup**

Parameters	Value
Routing Protocol	AODV
Simulation Time	20 s
No. of Mobile Nodes	40
Transmission Area	1300*1300
Mobility Model	Group Mobility Model
Type of Traffic	UDP
Data Packet Size	1024
Rate	5 mb/s
Speed Of a node	15 m/s
Proposed RREQ Rate Limit	10

## VI. RESULTS

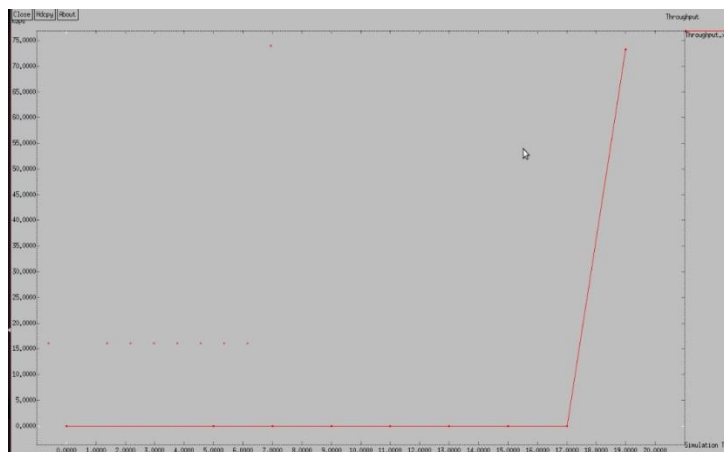
After simulation the proposed work, the graphs for the throughput, PDR and Overhead were obtained.

The figure 1 shows the simulation topology of the 40 nodes being simulated. The node 0 acts as the source node, nodes 1, 2, 4 and 12 from the first cluster. Nodes 5 and 10 act as the monitoring nodes for node 1, 2, 4 and 12 in which nodes 1, 2 and 4 are malicious nodes. Nodes 12, 11 and 15 are cluster heads for cluster 1, cluster 2 and cluster 3 respectively while as the destination node is represented by node 39.



**Figure 1: 40 Node Topology**

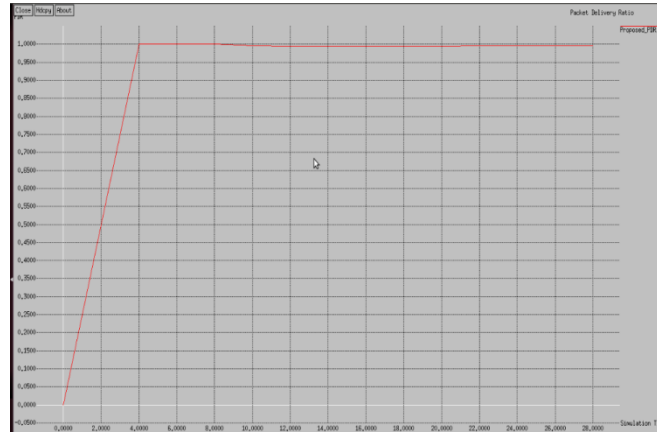
The figure 2 shows the throughput parameter of the proposed work.



**Figure 2: Throughput parameter vs Simulation Time**

At simulation time 0, 5, 7, 9, 11, 13, 15 and 17 seconds the value of throughput corresponds to zero and at 19 second of simulation time throughput abruptly increases to 73. 20 bits per second. It indicates that after completion of 19 seconds deployment of nodes at their respective positions takes place and every node starts communicating with their respective cluster heads, therefore the throughput of a particular network increases to 73. 20 bits per second.

The figure 3 shows the PDR parameter of the proposed work.



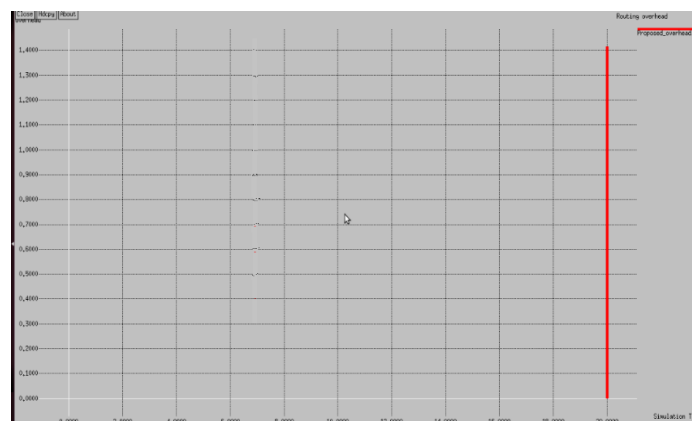
**Figure 3: PDR vs Simulation Time.**

The table below describes the value of PDR obtained at the corresponding simulation time.

**Table 2: Value of PDR with respect to Simulation Time**

Simulation Time (seconds)	PDR Value
4, 6, 8	1
10	0.9956
12	0.9946
14	0.9942
16	0.99428
18	0.9944
20	0.99448

The figure 4 shows the overhead parameter of the simulated network. At simulation time of 20 seconds the overhead value attained was 1.4139.



**Figure 4: Overhead vs Simulation Time**

## **VI. CONCLUSION AND FUTURE SCOPE**

To vitiate the performance of MANET, the Route Request Flooding Attack which comes under Distributed Denial of service attacks are foremost threat. A new approach is proposed which will efficiently defend from RREQ Flooding Attack in every applicable field. PDR is approximately equal to 1, Overhead equal to 1. 4139, and Throughput equal to 73. 20 which represents the qualities of efficient network scenario. The position of attacking nodes also plays important role on values of various metrics. If all malicious nodes are present in one cluster the performance degradation is more, as clustering overhead increases. For future research, a new method for clustering can be implemented on different routing protocols where battery power consumption, can be taken into account. Many other mobility models can be taken for testing in future research. Many other metrics can be taken into consideration for performance measurement. Moreover other applications can be taken into account as well.

## **VII. REFERENCES**

- [1]. JaydipSen, SripadKoilkonda, ArijitUkil, "A Mechanism For Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, IEEE page no. 238-343.
- [2]. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
- [3]. MeghnaChhabra, Brij Gupta, AmmarAlmomeni, "A Novel Solution to Handle DDOS Attack in MANET", Journal of Information Security, 2013, 4, 165-179.
- [4]. S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE. Wireless Commun. And Networking Conf., New Orleans, LA, 2005.
- [5]. TaranpreetKaur, Amanjot Singh Toor, Krishan Kumar Saluja, "Defending MANETs against Flooding Attacks for Military Applications under Group Mobility", Proceedings of 2014 RA ECS VIET Panjab University Chandigarh, 06 – 08 March, 2014, IEEE
- [6]. Ping Yi, Zhouli. n Dai, Shiyong Zhang, YipingZhong, "A New Routing Attack in Mobile Ad Hoc Networks", International Journal of Information Technology Vol. 11 No. 2, page no. 83-94.
- [7]. MeghnaChhabra and B. B. Gupta, "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)" Research Journal of Applied Sciences, Engineering and Technology 7(10): 2033-2039, 2014 ISSN: 2040-7459; e-ISSN: 2040-7467 page no 2033-2039.
- [8]. AlokparnaBandyopadhyay, Satyanarayana, Vuppala, Prasenjit Choudhury, "A Simulation Analysis of Flooding Attack in MANET using NS-3", 978-1-4577-0787-2/11/\$26. 00 ©2011 IEEE.
- [9]. Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "DoS Attacks in

- Mobile Ad-hoc Networks: A Survey”, 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE page no 535-541.
- [10] Y-C. HU, A Perrig and D. B. Johnson, ” Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks” *Wireless Networks* 11, 21–38, 2005 Springer Science & Business Media, Inc. Manufactured in The Netherlands.
- [11] Nadia Qasim, Fatin Said, and Hamid Aghvami, “Performance Evaluation of Mobile Ad Hoc Networking Protocols”, Chapter 19, pp. 219-229.
- [12] P. Ferguson, D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2267, January 1998.