International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 5 1119– 1125

A Modified AODV-Mechanism to Prevent Root Request Flooding Attack in Mobile Adhoc Networks

Er. Nitin Mohil
Electronics & Communication Engineering
ISTK, Kurukshetra University, Kurukshetra
Haryana, INDIA
mohil73.nitin@gmail.com

Ms. Kanta Dhankhar
Computer Science Engineering
ISTK, Kurukshetra University, Kurukshetra
Haryana, INDIA
kanta.dhankhar@gmail.com

***Abstract*—** A wireless Ad hoc Networks are highly pregnable to attacks due to their ingrained characteristics like absence of infrastructure and central administration, various types of Denial of Service Attacks (DoS) are possible because of the ingrained weakness of its routing protocols. The attacker node broadcast huge amount of fake Route Requests (RREQs) with fake destination address can lead to denial of service to genuine nodes. These attacks are not easy to detect because catty nodes copy normal nodes in all sense besides they do route discoveries much more frequently than the normal nodes. In this paper, we proposed a Modified AODV Mechanism to prevent Root Request (RREQ) Flooding Attack. The Denial of service attack stimulated due to RREQ Flooding attack in MANETs can be successfully prevented in the proposed Modified AODV Mechanism, the catty node identified as malicious are blacklisted for fixed time after timeout, it is allowed to take part in the network functionality.

Keywords*-MANETs,RREQ,Flooding,AODV,Modified AODV.*

*****

I. INTRODUCTION

A mobile ad hoc network (MANET) is a group of dynamic wireless nodes that can exchange information directly or indirectly through any intermediate node using dynamic routing without the use of any fixed or predefined infrastructure in which each device or node work as a router.
Most mobile devices use radio or infrared frequencies for their communications which leads to a very limited transmission range. Usually the transmission range is increased by using multi-hop routing paths. In that case a device sends its packets to its neighbour devices, i.e. devices that are in transmission range. Ad-hoc networks are temporary networks because they are formed to fulfil a special purpose and cease to exist after fulfilling this purpose. Mobile devices might arbitrarily join or leave the network at any time, thus ad hoc networks have a dynamic infrastructure [7].

In wireless networks [5], signals are transmitted via open and shared media. Without protection, anyone in the transmission range of the sender can intercept the sender's signal. Therefore, wireless communications are inherently less secure than their wired counterparts. Furthermore, wireless (mobile) devices usually have limited bandwidth, storage space, and processing capacities. It is harder to reinforce security in wireless networks than in wired networks.
There is no single mechanism that will provide all the security services in MANETs. The common security services are described as Availability, Confidentiality, Integrity, Authentication, Non repudiation, Anonymity, Authorization and Accounting [8].

- Availability: Availability states that services and resources must be provided to authorize nodes at all the time. There should be certain mechanism for detection and protection against such kind of attacks, which makes the network resources unavailable to authorized users like in case of DOS (Denial of service) attack, the availability of network and its resources, would become unavailable to legitimate user.

- Confidentiality: Confidentiality refers to hiding of information from unintended receivers.

- Integrity: Integrity refers to delivery of message to the intended recipient as such without any modification or alteration.

- Authentication: Authentication refers to verifying that the information is coming from a legitimate user.

- Non repudiation: Non repudiation ensures that sending and receiving parties can never deny ever sending or receiving the message.

- Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

- Authorization and Accounting: Nodes participating in a network need to have proper authorization to access shared assets on that network.

Routing in Mobile ad-hoc networks is one of the central tasks which help nodes send and receive packets. The purpose of routing in a MANET is to discover the most new topology of a continuously changing network to find a correct route to a specific node. In other words with routing a source node finds out the most fresh route to its destination node.

There are several type of routing protocol have been proposed, we can categorize them in to Reactive and Proactive routing protocols, reactive protocols are AODV, DSR etc and proactive protocols are DSDV, OLSR etc.

The whole paper comprises of six sections, the 1st section provides the introduction, 2nd provides information regarding the related work done to prevent RREQ flooding attacks,3rd section provides the information about the Normal Working of Ad-hoc on demand distance vector (AODV) Routing Protocol, 4th section provides the overview to the RREQ flooding attack, 5th section provides the information regarding the Modified AODV Mechanism to prevent RREQ flooding Attacks, 6th section provides the information regarding the Simulation Environment & Results and the 7th section provides conclusion to the whole paper.

II. Related Work

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato [2], proposed a new prevention scheme for the flooding attack in MANETs; in which each node maintain a count table for rate of RREQ of its neighboring nodes. If the rate of RREQ is more than predefined threshold value then the ID of that neighbor is blacklisted, but the limitation of this scheme is that it cannot prevent the attack in which rate of RREQ is below threshold.

Saman Desilva Rajendra, V. Boppana [11], proposed a mechanism to investigate the impact of hacker attacks by malicious nodes on the overall network performance. These malicious nodes mimic normal nodes in all aspects except that they do route discoveries much more frequently than the other nodes. We show, using simulations that the basic route discovery mechanism used in many ad hoc network protocols can be exploited by as few as one malicious or compromised node to bring down the throughput dramatically.

Arunmozhi Annamlai,Venkataramani Yegnanarayan [1], proposed a new defense scheme against the RREQ flooding attack. This paper focuses on mobile ad hoc network's routing vulnerability and analyzes the network performance under two types of attacks, flooding attack and black hole attack that can easily be employed against the MANETS. The resistive schemes against these attacks were proposed for Ad hoc on demand Distance Vector (AODV) routing protocol and the effectiveness of the schemes is validated using NS2 simulations.

Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao [9], proposed a new prevention scheme for RREQ flooding attack. This paper addresses few related works done on trust evaluation and establishment in ad hoc networks. Related works on flooding attack prevention are reviewed. A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment**.** The performance of the trust algorithm is tested in an ad hoc network implementing the Ad hoc On-demand Distance Vector (AODV) protocol.

III. Normal AODV Protocol

Ad-hoc on-demand Distance Vector routing protocol [12] uses on-demand route discovery technique to ensure loop free, single path, hop by hop distance vector routing. AODV operates in two sub phases. Route discovery Phase is initiated by a source node not having valid route to a destination node to which it wants to send data. Route maintenance phase for handling dynamic topology in MANET changes as the node moves or when some error persists. When a node wishes to send data to some destination it floods Route Request (RREQ) messages to all its neighbouring nodes. An intermediate node receiving RREQ updates its routing table with reverse route entry to the source node if RREQ is unique. Source id and broadcast id determines uniqueness of a RREQ packet. An intermediate node can further rebroadcasts RREQ to its neighbours or unicasts RREP message back to the source node if it already has unexpired route to that destination in its routing table otherwise destination node replies.

A. Protocol Overview [3][4]

Ad Hoc On-Demand Distance Vector, [RFC 3561], is a reactive routing protocol that is based on the Bellman-Form algorithm and uses originator and destination sequence numbers to avoid both “loops” and the “count to infinity” problems that may occur during the routing calculation process. AODV, as a reactive routing protocol, does not explicitly maintain a route for any possible destination in the network. However, its routing table maintains routing information for any route that has been recently used within a time interval; so a node is able to send data packets to any destination that exists in its routing table without flooding the network with new Route Request (RREQ) messages. In this way, the designers of AODV tried to minimize the routing overhead in the network caused by the frequent generation of routing control messages.

A third characteristic of AODV is its ability to interconnect nodes in a “pure” MANET running AODV with other non-AODV routing domains, thus extending any network with fixed infrastructure to a network with both mobile wireless nodes and static nodes, e.g., Ethernet.

A fourth characteristic of AODV is its support for both unicast and multicast routing. A final important characteristic of AODV is its ability to support both bidirectional and unidirectional links, as in many cases in wireless communications, two nodes in the network may only communicate with unidirectional links.

B. AODV Messages [3][4]

Three types of messages are used for route-discovery and link-failure notification: Route Request (RREQ) message, Route Reply (RREP) message, and Route Error (RERR) message. When a sender node does not have a valid route to a destination node in its routing table, it broadcasts a RREQ message.

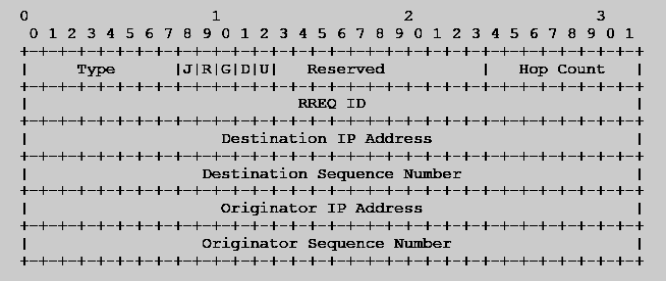

Figure 1. AODV Route Request Message Format [RFC 3561]

 ISSN: 2321-8169
1119– 1125

The destination node, or any intermediate node with a valid route to the destination, replies to the RREQ message with a RREP message. The RERR message is sent by a node to notify other affected nodes when a link failure is detected. Figures 1, 2, and 3 show the formats of the above three messages.

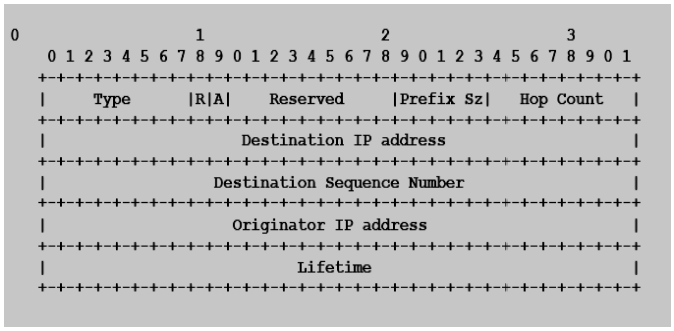

Figure 2. AODV Route Reply Message Format [RFC 3561]

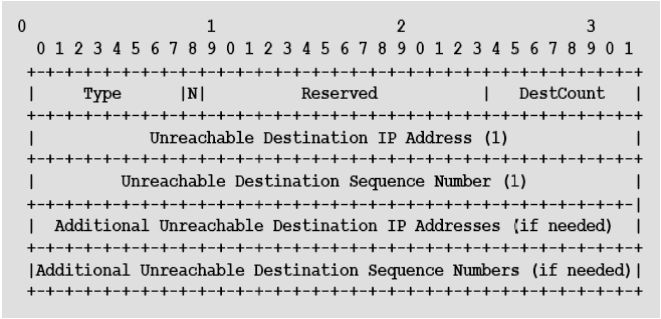

Figure 3. AODV Route Error Message Format [RFC 3561]

C. Route Discovery and Maintenance [4]

When a node, called "the originator," has data to send to another node in the network, called "the destination," the originator looks in its routing table to find a route to the destination

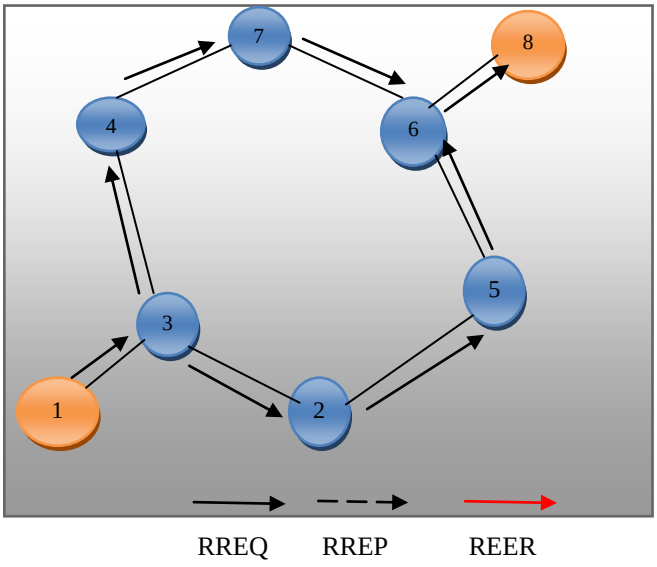

Figure 4. AODV Route Discovery Process

If there is no such route, or the route is marked as invalid by an appropriate flag, the originator propagates a RREQ message to its neighbouring nodes. The originator, before sending the RREQ message, increments by one the RREQ ID and the originator sequence number in the message header. In this way, each RREQ message is uniquely identified by combining the above numbers with the originator IP address. Any intermediate node that receives an RREQ message, takes one of the following three actions: First, the intermediate node discards the RREQ message if it has previously received the same RREQ message.

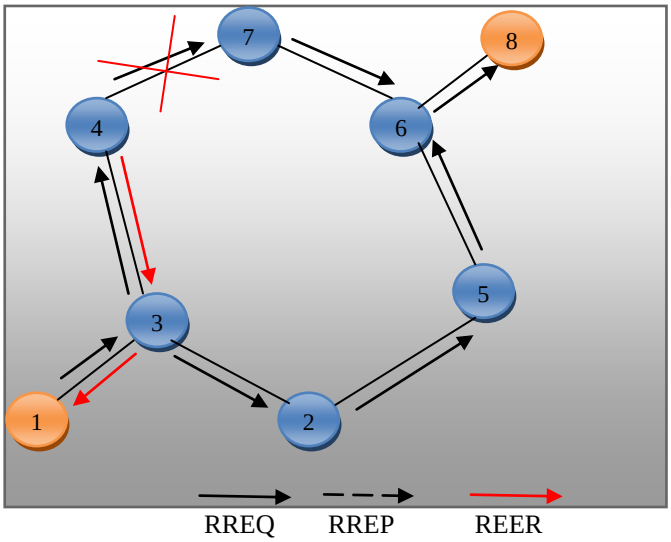

Figure 5. AODV REER Message Generations

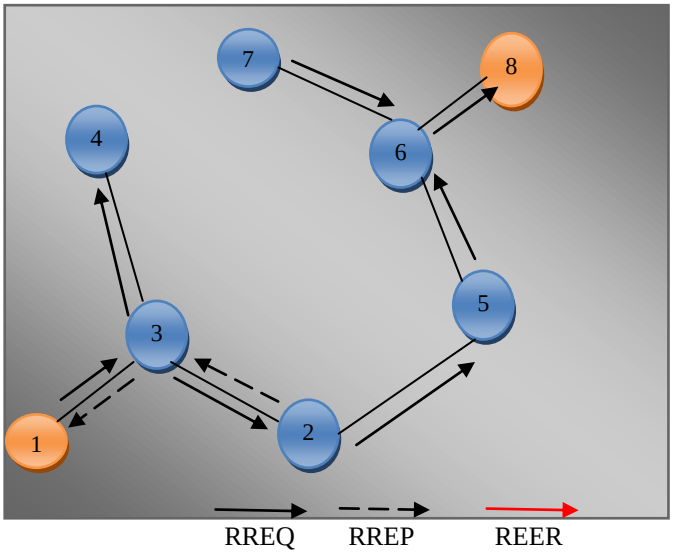

Figure 6. AODV Route Maintenance Process

AODV uses mainly two mechanisms to avoid high routing overhead caused by its flooding nature. The first mechanism involves a binary exponential back off to minimize congestion in the network. The second one involves an expanding ring search technique in which the originator node starts broadcasting a RREQ message and the TTL value is set to a minimum default value. If the originator node does not receive a RREP message within a certain time interval, it

exponentially increments the time interval and increases the diameter of the searching ring. The maximum value for the ring diameter is set by default to 35, which is, for AODV, the maximum value of the network diameter.

The route maintenance process in AODV is very simple. When the link in the path between node 1 and node 8 breaks (Figure 5) the upstream node that is affected by the break, in this case node 4 generates and broadcasts a RERR message. The RERR message eventually ends up in source node 1. Upon receiving the REER message, node 1 will generate a new RREQ message. Finally, if node 2 already has a route to node 8, it will generate a RREP message, as indicated in Figure 6. Otherwise, it will re-broadcast the RREQ.

IV. Root Request Flooding in AODV Protocol

AODV routing protocol is vulnerable to RREQ flooding attack [6][10] because of the route discovery scheme and its broadcast mechanism. To reduce congestion, the protocol has already adopted some methods which are briefly described as follows. In AODV there is limit of how much RREQ can be originated by a node. The default value of RREQ_RATELIMIT is 10 as proposed by RFC 3561. Secondly, after broadcasting a RREQ, the initiator will wait for a ROUTE REPLY.-If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, until it reaches a maximum of retry times at the maximum TTL value. Time intervals between repeated attempts by a source node at route discovery for a single destination must satisfy a binary exponential backoff. The first time a source node broadcasts a RREQ, it waits round-trip time for the reception of a ROUTE REPLY. Malicious node would exploit this weakness and initiate much more RREQ packets than the normal node in order to consume the network or victims resource. The RREQ packets are given more priority than the data packets; the nodes spend more time in processing the RREQ packets and there by delay the service for the legitimate users. A malicious node can override the restriction put by RREQ_RATELIMIT (limit of initiating or forwarding RREQs) by increasing it or disabling it. A node can do so because of its self-control over its parameters. A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a very high number. This allows it to flood the network with fake RREQs and leads to a kind of DoS attack. In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. This will not only lead to the exhaustion of the network resources like memory (routing table entries), but also lead to the wastage of bandwidth and the wastage of nodes' processing time.

V. Modified AODV Mechanism to Protect Root Request Flooding Attack

The proposed algorithm uses a filter to detect malicious node and reduces their impact on network performance. The aim of the filter is to limit the rate of RREQ packets. Each node maintains a threshold value which serves as the criterion for each node's decision of how to react to a RREQ message.

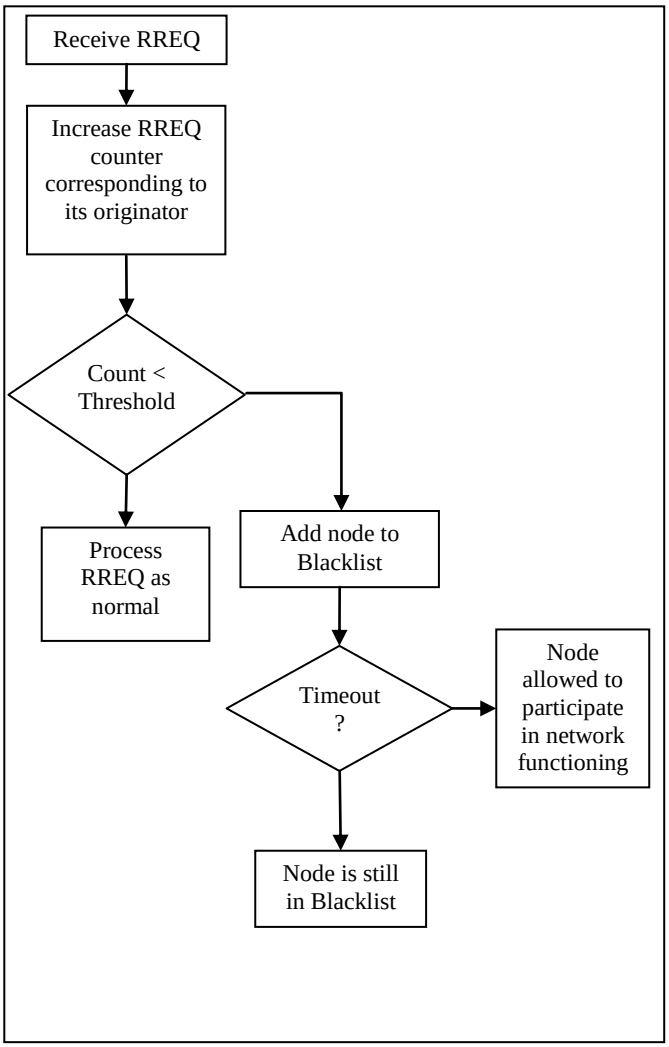

Figure 7. Modified AODV Mechanism against RREQ Flooding Attack

The threshold parameter denotes the number of RREQs that can be accepted and processed as normal per unit time by a node. Each node monitors the route requests it receives and maintains a count of RREQs received for each RREQ originator during a preset time period. Whenever a RREQ packet is received, a check is performed. If the rate of this RREQ originator is below the threshold, the RREQ packet is processed as normal.

The threshold value specifies a value that aids in determining whether a node is acting malicious or not. If the number of RREQs originated by a node per unit time exceeds the value of threshold, one can safely assume that the corresponding node is trying to flood the network with possibly fake RREQs. On identifying a sender node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network. The blacklisted node is ignored for a period of time after which it is unblocked to support dynamic nature of mobile ad hoc networks. After that it is allowed to take part in the network functionality. If it again misbehaves, timeout will increase. The neighboring nodes of the malicious node are therefore free to entertain the RREQs from other genuine nodes. In this way genuine nodes are saved from experiencing the DoS attack.

ISSN: 2321-8169
1119– 1125

VI. Simulation Environment & Results

This section describes the scenario with all the network parameter, which is used for simulation. NS-2[13] simulator is used for this simulation study. This study considers three cases: AODV, AODV under RREQ flooding attack and our proposed algorithm. In the sample scenarios, traffic source is Constant-Bit-Rate (CBR) and the field configuration is 1000×1000 m with varying number of nodes from 15 to 45 and pause time from 1sec to 10 sec. Table I shows the simulation parameters and their respective values, which are used to examine the performance of the network.

Table I: Simulation Parameters

Parameter	Value
Simulation time	150 Sec
Simulation area	1000m x 1000m
Antenna	Omni antenna
Packet size	512 Bytes
Max queue length	50
Traffic	CBR (Constant bit rate)
Transport Layer	UDP
Speed	10 m/s
Data Rate	8 packets per second

Performance Metrics

Different performance metrics are used in the evaluation of routing protocols. They represent different characteristics of the overall network performance. In this report, we evaluate four metrics used in our comparisons to study their effect on the overall network performance. These metrics are network throughput and Normalize Routing Load.

Throughput

The ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput in MANETs include frequent topology changes, unreliable communication, limited bandwidth and limited energy. A high throughput network is desirable.

Normalize Routing Load (NRL)

It is the ratio of the number of routing packets transmitted to the data packets delivered.

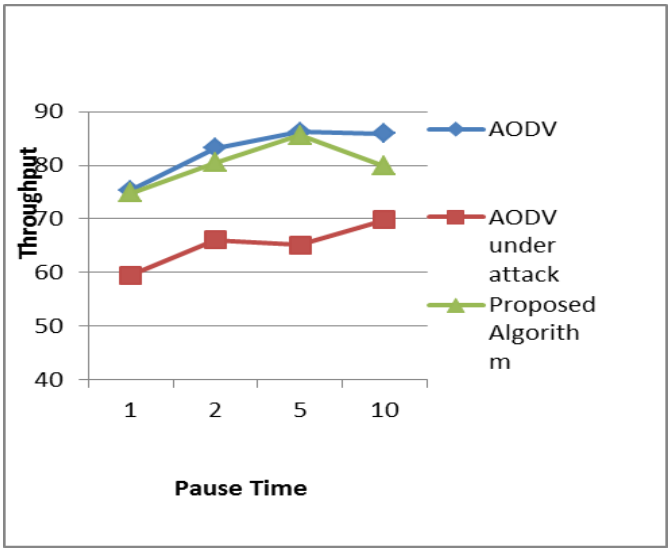

Figure 8. Throughput vs. Pause Time

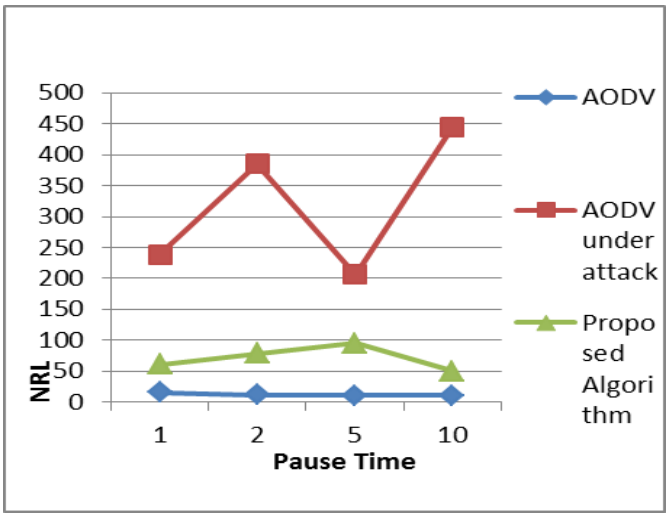

Figure 9. NRL vs. Pause Time

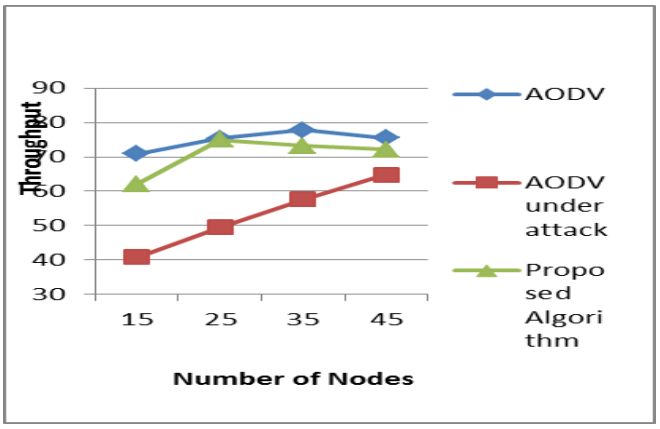

Figure 10. Throughput vs. Number of Nodes

 ISSN: 2321-8169
1119– 1125

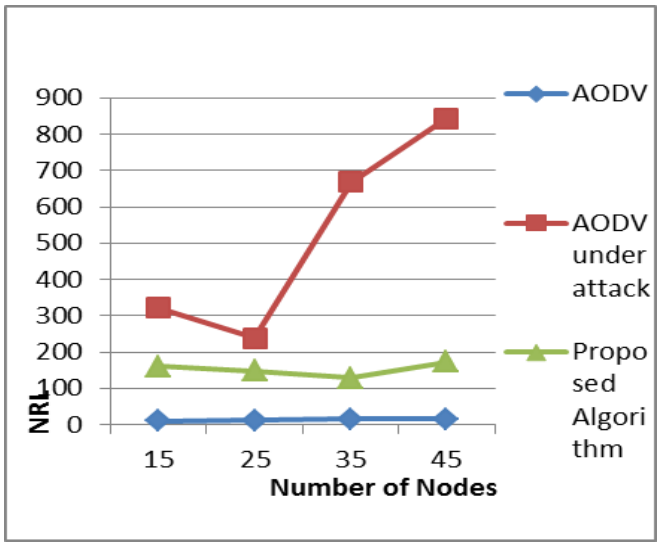

Figure 11. NRL vs. Number of Nodes

Figure 8:
We have simulated the network using Normal AODV, AODV under RREQ flooding attack and proposed mechanism. It shows the performance in terms of throughput. As pause time varies the throughput of the network decreases under RREQ Flooding attack 75.34 kbps to 59.46 kbps and it rises to 74.88 kbps with our proposed mechanism..

Figure 9:
We have simulated the network using Normal AODV, AODV under RREQ flooding attack and proposed mechanism. It shows the performance in terms of Node Routing Load (NRL). As pause time varies the NRL of the network increases under RREQ flooding attack 15.52 to 238.9 and it decreases to 60.79 with our proposed mechanism.

Figure 10:
We have simulated the network using Normal AODV, AODV under RREQ flooding attack and proposed mechanism. It shows the performance in terms of Throughput. As No. of Nodes varies the Throughput of the network decreases under RREQ flooding attack 70.89 kbps to 40.89 kbps and it rises to 62.05 with our proposed mechanism.

Figure 11:
We have simulated the network using Normal AODV, AODV under RREQ flooding attack and proposed mechanism. It shows the performance in terms of Node Routing Load (NRL). As No. of Nodes varies the NRL of the network increases under RREQ flooding attack 10.19 to 320.69 kbps and it decreases to 127.71 with our proposed mechanism.

VII. CONCLUSION

In this paper, we analyzed the effect of RREQ Flooding Attack on AODV Network. Although several methods have been proposed to prevent RREQ flooding attack but every mechanism have their own advantages and shortcomings. Here we have analyze the effect of Root Request (RREQ) Flooding Attack on performance metrics Throughput and Node Routing Load with variation in pause time and No. of nodes as shown in Table II and Table III.

Table II: Effect of varying pause time on performance metrics

Parameter / Mechanism	Throughput	NRL	Variations in Pause Time
AODV	75.34 to 85.93	15.52 to 9.99	1,2,5 & 10
AODV under RREQ Flooding Attack	59.46 to 69.86	238.9 to 445.55	1,2,5 & 10
Proposed Mechanism	74.88 to 79.9	60.79 to 50.13	1,2,5 & 10

Table III: Effect of varying number of nodes on performance metrics.

Parameter / Mechanism	Throughput	NRL	Variations in No. of Nodes
AODV	70.89 to 77.73	10.19 to 14.16	15,25,35 & 45
AODV under RREQ Flooding Attack	40.89 to 64.78	320.69 to 842.9	15,25,35 & 45
Proposed Mechanism	62.05 to 74.88	127.71 to 172.02	15,25,35 & 45

To evaluate the effect of varying pause time on performance metrics, simulation is done with 25 nodes with source node transmitting 8 packets per second and flooding rate is 0.07. Each packet is of 512 bytes.
As it can be seen from the figure 8, Flooding attack reduces throughput by 21.60%. Excessive flooding of RREQs in the network causes congestion in the network which leads to more packets dropped as compared to normal AODV and decreased throughput.

NRL increases from 10.19 in AODV without attack to 320.29 with attack as shown in figure 9, NRL of proposed algorithm is close to normal AODV, thus our scheme does not cause much routing overhead.

As number of node increases from 15 to 45, throughput of the network increases as shown in figure 10. AODV under attack lowers the throughput of the network by 42.46%. With the proposed scheme it increases from 62.05 kbps to 74.88 kbps which is very close to normal AODV.

NRL also increases with increasing node as more control messages are exchanged in the neighborhood. NRL of normal AODV ranges from 10.19 to 14.6 and under attack it varies from 320.69 to 842.9 and with our scheme it drops to 127.71 with varying number of nodes, depicted in figure 11.

From the above cases, we can conclude that Modified AODV mechanism give significant improvement in Throughput and NRL or same as normal AODV compared to that of AODV during RREQ Flooding attack.

So looking at all the results we can conclude that Modified AODV mechanism to prevent RREQ Flooding Attack gives better performance or same as normal AODV compared to an AODV under RREQ Flooding attack.

REFERENCES

[1] Arunmozhi Annamlai, Venkataramani Yegnanarayan, ”Secured System against DDoS Attack in Mobile Adhoc Network,” WSEAS Transaction on Communication Issue 9, Volume 11, September 2012.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, “A Survy of Routing Attacks in Mobile Ad hoc Network,” IEEE Wireless Communications, October 2007..

[3] C. Perkins, E. Belding-Royer,” Ad hoc On-Demand Distance Vector (AODV) Routing”, IETF July 2003.

[4] Kioumourtzis, Georgios A.,”Simulation and evaluation of routing protocols for Mobile Ad Hoc Networks (MANETs),” Monterey, California. Naval Postgraduate School, September 2005.

[5] Klara Nahrstedt, Wenbo He, and Ying Huang,” Security in Wireless Ad Hoc Networks,” Guide to Wireless Ad Hoc Networks, Sudip Misra, Isaac Woungang, Subhas Chandra Misra (Eds.) pp 401-435, @2009 Springer.

[6] Meghna Chhabra, Brij Gupta, Ammar Almomani,“A Novel Solution to Handle DDOS Attack in MANET,” Journal of Information Security, July 2013.

[7] Nitin Mohil, Kanta Dhankhar, “Survey of Detection and Prevention Mechanism for Flooding Attacks in MANETs,” International Journal of Research in Advent Technology, Vol.2, No.5, May2014.

[8] Nitin Aggarwal, Kanta Dhankhar,”Attacks on Mobile Adhoc Networks: A Survey,” International Journal of Research in Advent Technology, Vol.2, No.5, May 2014.

[9] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao,”Performance Analysis of Flooding Attack Prevention Algorithm in MANETs,” World Academy of Science, Engineering and Technology 32, 2009.

[10] Sotirios E. Athanaileas, Christopher N. Ververidis and George C. Polyzos,” Optimized Service Selection for MANETs using an AODV-based Service Discovery Protocol,” The Sixth Annual Mediterranean Ad Hoc Networking WorkShop, Corfu, Greece, June 12-15, 2007.

[11] Saman Desilva Rajendra V. Boppana,”Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” IEEE Wireless Communications and Networking Conference, March 2005.

[12] Tarunpreet Bhatia, A. K. Verma, “Simulation and Comparative Analysis of Single Path and Multipath Routing Protocol for MANET,” Anveshanam - The Journal of Computer Science & Applications, VOL. II, NO. 1, August 2013-July 2014.

[13] www.isi.edu/nsnam/ns/