ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

RREQ Flooding Attack Mitigation in MANET Using Dynamic Profile Based Technique

Dr.T.Pandikumar[1], Habtewold Desta[2]
Associate Professor[1], M.Tech Student[2]
Department of Computer & IT
College of Engineering, Defense University, Debre Zeyit, Ethiopia

Abstract:
Mobile Ad-hoc Network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. These types of networks are more prone to attacks that occur in the network. As the demand for the MANETs are increasing day to day, due to the increasing demand for MANETs in various areas such as in Military operations and in flood affected areas, threat of security has also increased. The main challenge in MANET is to design the strong security solution that can protect MANET from various routing attacks. From those routing attack RREQ flooding attack is one. RREQ Flooding attack launched at network layer is a kind of Denial of service (DOS) attack which is distributive in nature and can exhaust the victim's network resources such as bandwidth, energy, computing power etc. The route discovery scheme in reactive routing protocols like Ad hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) used in MANET makes it easier for malicious nodes to launch connection request floods by flooding the route request packets (RREQ) on the network. In this paper we propose a Dynamic profile based technique (DPDS) which is used to mitigate the RREQ flooding attack on MANET using Ad hoc on Demand Distance Vector (AODV) routing protocol and we got 52.27 – 98 % Pdr for static node and 44.75 – 87.69 % Pdr for Mobile Nodes.

Keywords: Ad hoc on Demand Distance Vector (AODV), Dynamic Profile Based Technique (DPDS), Flooding Attack, RREQ Flooding Attack.

1. INTRODUCTION

The evolution of Mobile wireless Network has affect in the field of communication through its advantages such as the absence of physical media, the concept of mobility and the difficulty to use the wiring. In recent years, Mobile Ad hoc Network (MANET) has received marvelous attentions due to self-design, self-maintenance, and cooperative environments. Mobile Ad Hoc Networks (MANETs) are formed dynamically by an autonomous system of nodes that are connected via wireless links without using the existing network infrastructure [1]. It is infrastructure-less network in which nodes cooperate to forward data from a source to a destination. Thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion. Each node has a wireless interface and communicates with its neighbors who are all in its coverage range. Source can reach destination through one or multiple hop. MANET is a multi-hop wireless network where all mobile nodes are connected with each other working together to achieve their objective. This kind of networks does not need any centralized administration and there is no condition on its size. Each node can act as a host or as a router or both in the same time.

1.1 Statement of the Problem

Mobile Ad-Hoc Networks (MANETs) are impromptu wireless communication networks increasingly appearing in the Commercial, Military, and Private sector as portable wireless computers become more and more ubiquitous. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. This offers an advantageous decentralized character to the network. Decentralization makes the networks more flexible and more robust. Since the network topology changes frequently, efficient adaptive routing protocols such as AODV, DSR are used. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission. Most of the reactive protocols like AODV are prone to flooding attacks which is a kind of denial of service attacks during their route discovery process. A malicious node may actively involve in the flooding attack by repeatedly sending RREQ or garbage data packets to different destinations some of which never exists. A neighboring victim node may drain its resources like battery power, consuming bandwidth, processing time by involving itself in the routing traffic.

1.2 Scope of the Study

This thesis work mainly focuses on simulation study of RREQ flooding attack and its prevention mechanism in AODV routing protocol. Flooding attack by other control packets other than RREQ packet is not studied. This thesis work has improved the communication of Mobile ad-hoc network.

1I. ROUTING PROTOCOLS IN MANET

2.1 Introduction

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a

destination node might be out of range of a source node transmitting packets; a routine procedure is always needed to find a path so as to forward the packets appropriately between the source node and the destination node. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of MANET, each node must be able to forward data for other nodes. In MANET nodes requires routing protocol to reach destination, as nodes may or may not be in range requires routing in multiple hops. So the nodes depend on one another for transmission of packets from source nodes to destination nodes via the routing nodes. The aim of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node [1]. Routing protocols for MANET networks can be classified into three types based on the underlying routing information update mechanism employed. An ad-hoc routing protocol could be reactive (on demand), proactive (table driven) or hybrid [5, 6, 33]. Figure 1 shows the three types of MANET routing protocols and some list of the available routing protocols for that category.

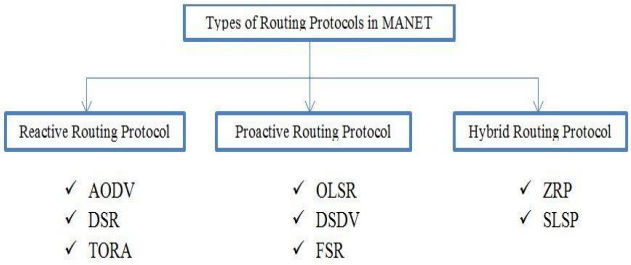

Figure. 1. Types of Routing Protocol

Hybrid Protocol, this protocol has the properties of both proactive and reactive protocol. Since nodes in an ad hoc network move quite fast, and as the changes may be more frequent than the route requests, most of this routing information is never even used! This results in a further waste of the wireless network capacity. What is needed is a protocol that, on one hand, initiates the route determination procedure on-demand, but at limited search cost. The protocol described in this draft, termed the "Zone Routing Protocol (ZRP)".

2.2 Ad Hoc on Demand Distance Vector Routing (AODV)

According to Mahesh K. Marina (2006) :Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi hop routing, dynamic topology maintenance, Loop-free, Low consumption of memory, bandwidth, Scalable to large node populations, Minimal overhead for data transmission, Rapid convergence and Multicast between participating mobile nodes wishing to establish and maintain an ad hoc network.

AODV allows MANET nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in network range. There are three message used by AODV namely Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs). Detail descriptions of these messages are discussed in detail in draft of AODV, RFC 3561.

Route Request (RREQ) Message This message is sent from source to destination to get connected and transfer data from source to destination. Fig 2 shows the RREQ message formats.

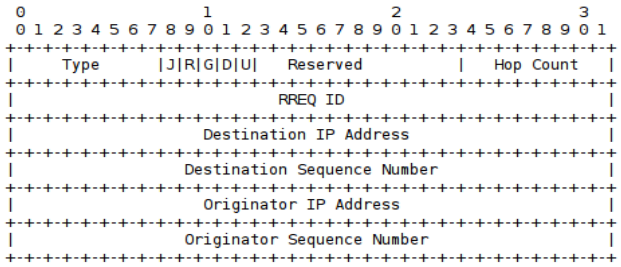

Figure 2. RREQ Message Format

I1I. METHODOLOGY

This chapter depicts the methodology to implement RREQ flooding attack behavior under AODV routing protocol and its mitigation techniques using dynamic profile based technique. Before that, the network simulator and the implementation of AODV in NS-2 are discussed.

3.1 Network Simulator 2 (NS2)

As different papers review indicates there are many network simulators with different features and NS-2 is one of the most popular open source network simulators. Network Simulator (Version 2) is widely known as NS2. It is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community.

NS2 is a discrete-event simulator, where actions are associated with events rather than time. An event in a discrete-event simulator consists of execution time, a set of actions, and a reference to the next event. These events connect to each other and form a chain of events on the simulation timeline. Unlike a time-driven simulator, in an event-driven simulator, time between a pair of events does not need to be constant.

3.2 Cloning AODV Protocol

To integrate RREQ flooding attack into AODV, cloning AODV protocol were necessary. To clone AODV protocol properly we undergo serious of procedures. It has serious issue if the cloning goes in inappropriate way. So that we cloned AODV protocol to FAOD as we putted a procedure in Appendix section.

3.3 Modeling of Flooding Attack

In this case the attacker selects a destination that does not exist in the network. Then it builds the RREQ message and simply floods the request without even checking the routing table for the route. After receiving the RREQ from the attacker, the intermediate nodes try to look the route for the destination in their routing table and finally flood the request to their respective neighbors as none of the nodes has a route to the destination. The attacker waits for some interval, the interval in our case 0.07 second, which controls the rate of flooding, and starts the flooding again. This flooding interval is varied during the simulation. The way of RREQ flooding attack can be summarized as in the following figure 3.

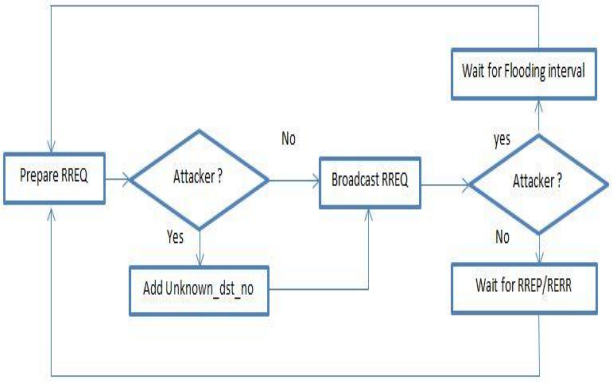

Figure .3. Modeling RREQ flooding attack

3.4 RREQ Flooding attack integration in NS2

It is known that, all routing protocol in NS2 are installed in directory called ns-allinone-2.35/ns-2.35/. In this directory there is a cloned version of aodv called faodv, which is created by the above procedure. So that to integrate RREQ flooding attack behavior in to faodv protocol we make some changes in faodv.cc and faodv.h file. Here is the procedure how to create a RREQ flooding attack on AODV or in our cloned name FAODV protocol. Before we create we have to consider that how many packets should be sent over the network per node per second. This will help as to know how many RREQ packets are flooding the network per second.

3.5 Prevention Mechanism of RREQ flooding attack

As we see from the behavior of the attack. The attacker uses unknown node id so that it broadcasts to unknown destination to consume the battery power, bandwidth and energy of a node. The prevention mechanism is little bit tricky.

3.6 Dynamic Profile Based Detection Scheme

The proposed detection scheme (DPDS) Dynamic Profile based Detection Scheme aims at detecting the flooding attack on MANET. The DPDS approach uses dynamic profile based traffic analysis to mitigate misbehaving nodes. The DPDS approach has two phases of operations detection phase and isolation phase. The DPDS system will have set of modules which try to quantify the normal behavior of the nodes and identify the abnormal behavior of the malicious node. In Normal mode: This mode collects the details about the normal operation of AODV like sending request receiving request. Here the RREQ broadcast mechanism adheres to the rate limit parameter in sending the RREQ packets. According to RFC-3561 any legitimate node can send up to 10RREQ/sec [6]. The details in terms of network parameters are collected by the performance mode.

3.7 Design of the Prevention Mechanism

The RREQ flooding attack occurs at the route discovery stage. So as we propose we first look for the profile of each node. To do this, the average number of route request RREQ per second will be calculated and finally this average RREQ value will be used to calculate RATE_LIMIT to dynamically estimate the threshold value. This estimated threshold value can be used to detect misbehaving nodes below the known threshold value as well as above the threshold. The receiving procedures are modified and are described as follows.

3.7.1 Receiving Route Request

Let's look at normal operation of the protocol. When an intermediate node receives route request, from its neighbor it checks for the freshness of the information and caches the request and sets up the reverse path back to the originator. If the receiving node is an intermediate node with fresh route to the destination or if the receiving node is the destination itself, then it sends the reply to the originator of the RREQ message. Otherwise the request is forwarded to its neighbors.

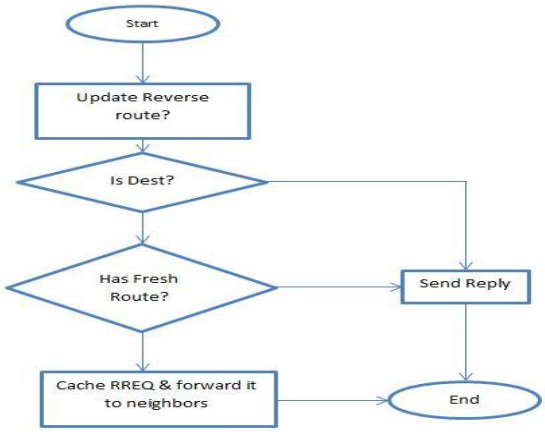

Figure. 4. RREQ Receiving In AODV

The proposed approach as described in figure 4 tries to minimize unnecessary RREQ packet flooding and saving the battery power of legitimate node. This approach works on dynamic threshold value of RREQ packets and the threshold police. The Proposed technique is based on profile maintained for previous recorded RREQ packets in certain number of sessions at time of simulation. This approach is based on finding the RREQ packets received by each intermediate node from their neighbor source nodes in sessions maintained in routing table. Then average of RREQ packets received per second in all session is calculated. Rate Limit is also calculated based on this average value. Profile is maintained on each node which contain record the RREQ packets values in the sessions created during simulation and by applying formula for nodes discard limit and average value is calculated.

IV. RESULT AND ANALYSIS

This chapter discusses the normal AODV protocol operation, performance and the effect of RREQ flooding attack on AODV routing protocol. It also discusses about the efficiency of the mitigation technique by applying dynamic profile based technique AODV protocol. To evaluate the performance of mitigation technique as well as the effect of RREQ flooding attack we use different metrics like Packet Delivery Ratio, Average Throughput, link to link Delay and Packet Dropped Ratio. To analyze the effect of RREQ flooding attack deeply we categorize the simulation procedure in to moving mobile node and fixed mobile node. The result shows as how RREQ flooding attack is highly consuming the network bandwidth and the battery life of the nodes.

4.1 Simulation Procedure

Initially network with 22 and 30 nodes is created in a fixed location as well as in random location for movable nodes. When creating this network we assume the 1700 X 700m network scale. We use UDP (user datagram protocol) as it is a best way for communication which needs no acknowledgment. We didn't use a TCP protocol as it needs TCP-Ack for communication. Finally we use CBR (constant bit rate) agent for UDP communication.

4.2 Simulation Parameter

In this simulation, we simulated a network within 1700 X 700m range and 22 – 30 nodes. The nodes moves in random way point mobility and in fixed network they stay on statically given location. In both scenarios we use 1-6 malicious nodes for mobile node communication and 1-5 malicious nodes for static nodes communication. With 17 – 21 legitimate nodes for static nodes and 24-29 legitimate nodes for random mobile nodes. The main thing we use different number of legitimate and different malicious nodes are to see exactly how RREQ flooding attack affects and consumes the battery life of the legitimate nodes. We use 17 - 22 numbers of nodes for simulating static node communication network using AODV and its effect on RREQ flooding attack form 1-5 malicious nodes inside network. The same thing happens on movable nodes containing 24-29 legitimate nodes and 1-6 malicious nodes RREQ Flooding Attack Effect and performance of PDS Approach.

4.2.1 RPEQ Flooding Static nodes

This scenario shows exactly the effect of RREQ flooding attack. The aim of this scenario is to see how a malicious node can affect mobile nodes if they stand together for long period of time and to analyze the performance the proposed mitigation technique. As we tried to show the effect of RREQ flooding attack on route of nodes in Figure 6.9 the nodes tries different ways to reach the destination while malicious nodes are flooding them.

This means that the RREQ flooding attack also make the route mechanism of AODV too weak. Besides weakening the route mechanism, it also consumes the bandwidth of the networked mobile nodes and it decrease the packet delivery ratio of mobile nodes. After seeing all the DPDS approach highly enhance the route mechanism, the packet delivery ratio, throughput of mobile nodes and protect packet drops.

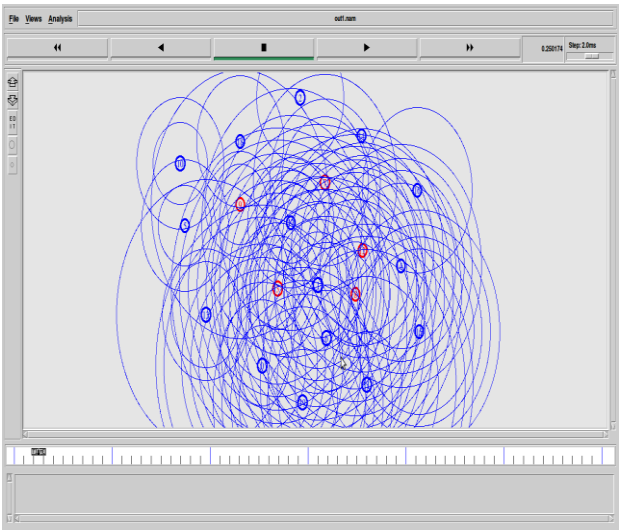

Figure .5. RREQ Flooding Static nodes

4.2.2 RREQ Flooding Mobile Nodes

It is vital that seeing the effect of RREQ flooding attack on mobile nodes. As we see below in the Figure 6 five malicious nodes are flooding the network while moving randomly.

To show the effect of RREQ flooding attack and its effect we have calculated the Packet delivery ratio, Throughput, End to End Delay and Packet Dropped per simulation. As the values shows RREQ flooding attack highly consumes network resources.

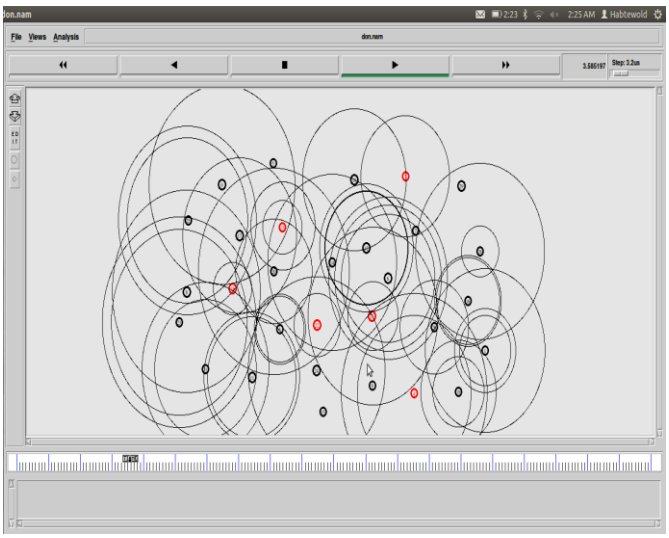

Figure .6. RREQ Flooding Mobile Nodes

4.2.3 End to End Delay

End to end delay is the time taken to a packet to reach its destination from source to destination and here the following table shows the end to end delay of packets from source to destination on the presence of attack and proposed mitigation technique is applied.

Can be calculated as End-end_d = N [Dtrans + Dprop + Dproc + dqueue] …….. (2)

Table .1. End to End Delays

Attacker	Flooded Mobile Node (EED)	DPDS Applied Mobile Node(EED)	Flooded Static Node (EED)	DPDS Applied Static Node(EED)
0	158.58	49.82	41.51	41.51
1	937.52	32.85	36.71	36.71
2	1450.17	31.44	596.72	36.20
3	979.16	38.61	1090.05	31.76
4	1837.35	32.31	1317.40	102.36
5	588.22	33.68	0.00	33.83
6	588.2	32.48	--------	--------

The following graph is the result of the above table 1.

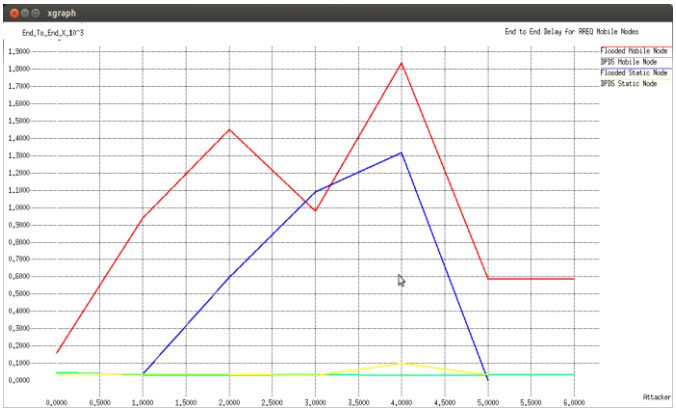

Figure .7. End to End Delays

4.2.4 Average Throughput

A throughput is said to be feasible/achievable if every node can send at a rate of maximum bits per second to its chosen destination. As described below we got good throughput in the presence of RREQ attack on network.

Table. 2. Average Throughputs

Attacker	Flooded Mobile Node (Kbps)	DPDS Applied Mobile Node(Kbps)	Flooded Static Node (Kbps)	DPDS Applied Static Node(Kbps)
0	17.93	14.68	16.00	16.00
1	13.71	16.16	16.02	16.02
2	8.96	13.92	14.74	16.02
3	3.76	14.51	10.21	15.34
4	1.83	12.29	5.85	15.65
5	3.29	8.77	0.39	8.47
6	3.29	13.82	--------	--------

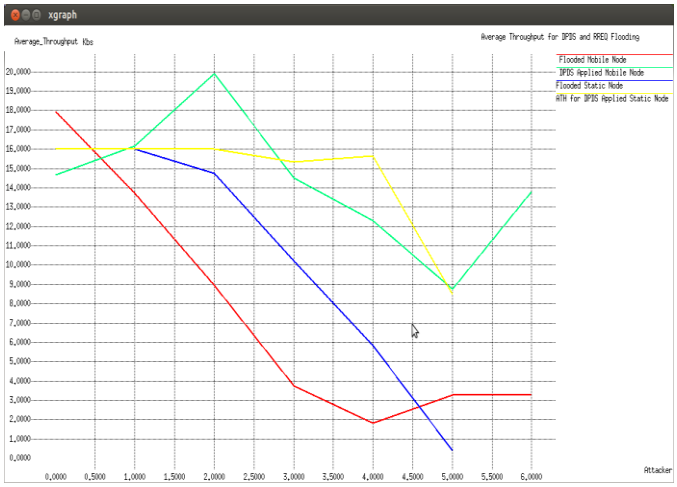

Figure. 8. Average Throughputs

This chapter deals about the detail implementation of the thesis project on NS2 simulator and results and analysis from implementation. In this stage we have include results from research. By reporting on the implementation, a clear picture is given of the research task and of the process through which we have sought to reach the goal of the research.

VI. CONCLUSION AND FUTURE WORK

One of the main challenges in mobile ad hoc network is to design the robust security solution that can protect MANET from various routing attacks. In thesis work we have investigated the impact and effect of RREQ flooding attack on AODV protocol. RREQ Flooding attack launched at network layer is a serious routing attack which can consume more resources like bandwidth, battery power, etc. It is also more concealed form of DOS and resource consumption attack. By using a Network Simulator 2(NS2) simulation environment, dynamic profile based detection technique is applied as proposed And Its effectiveness in detecting and isolating the malicious node that floods the route request packets is evaluated by using the evaluation metrics like; Packet delivery ratio, Average throughput, End to End Delay and Packet Drop Rate. When evaluating this we use two different scenarios with different number of mobile nodes and movement strategies. In the first scenario we used 22 numbers of nodes including attacker nodes and with varying number of attacker nodes from 1-5 attackers there was great number of packet loss in percent form 3.41% - 98.86 % packet loss where seen respectively. After Appling Dynamic Profile Based Detection scheme we got good result. In DPDS applied nodes with the presence of 1- 5 RREQ flooding attacker the packet loss is decreased by great number percent from 1.14% – 47.73%. In second scenario we use 30 numbers of mobile nods including varying number of attacker nodes from 1-6 attacker nodes. We get packet loss rate form 12.31- 55.26% to 30.03 – 97.30%. The DPDS approach detects the attacker as soon as the attacker starts exhibiting its attack behavior. PDS detects and isolates the attacker efficiently with better response time and do not engage much overhead.

6.1 Future work

Finally we concluded that the RREQ flooding attack effect on performance metrics. The Effect of the attack is clearly shown in PDR, end to end delay, packet drop rate and average throughput. As attacker node is the main security threat that effect the performance of the AODV routing protocol. Therefore, the proposed DPDS approach work do better to detect and defense the network from RREQ flooding attack.
In future this work can be further extended for other kind of flooding attacks with respect to AODV like hello packets; syn floods and data packets etc.

VII. REFERENCES

[1]. Abhishek Choudhary, Kunal (2012), "Performance Evaluation of AODV under Black hole Attack", IJETAE publication Volume 2, Issue 5, May 2012.

[2]. Amandeep (2012), "Performance Analysis of AODV Routing Protocol in MANETs", International Journal of Engineering Science and Technology (IJEST), Vol. 4, No.08, August 2012.

[3]. Anil G. N (2012), "Semantic Probabilistic Modeling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile ad hoc network", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[4]. B. B. Gupta, R. C. Joshi, and ManojMisra (2009), Member, IEEE "Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network", IJCTE publication Vol. 1, No. 1, April 2009.

[5]. Bhuvaneshwari .K, Dr. A. Francis SaviourDevaraj (2013), "ANP- Adaptive Node Profile Based Detection Mechanism for Flooding Attack in MANET", IJERT publication Vol. 2 Issue 3, March – 2013.

[6]. Bhuvaneshwari .k, Dr.A.FrancisSaviourDevaraj (2013), "PDS- A Profile based Detection Scheme for flooding attack in AODV based MANET". IJSPTM publication Vol. 2, No.3, June 2013.

[9]. Charushila Choube, M. Murali (2015), "Detection of Route Request Flooding Attack in MANET Using Session Based History Table", IJISET - International Journal of Innovative Science, Engineering & Technology publication. Vol. 2 Issue 4, April 2015.

[10]. Er. Nitin Mohil, Ms. KantaDhankhar (2014), "Survey of Detection and Prevention Mechanism for Flooding Attacks in

MANETs". International Journal of Research in Advent Technology publication Vol.2, No.5, May 2014.

[11]. H. Kim, (2010), " Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks ", IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010.

[14]. Kartik Kumar Srivastava, Avinash Tripathi, Anjnesh Kumar Tiwari (2013), "Secure Data Transmission In AODV Routing Protocol" Computer Science & Engineering Institute of Technology & Management GIDA, Gorakhpur 04 April 2013.

[15]. Khushboo Sharma, Anurag Jain, "The performance evaluation of Adjusted Probabilistic Flooding on AODV protocol based on flooding mechanism in MANETs" IJACT publication.

[16]. Mahesh K. Marina (2006), "Ad hoc on-demand multipath distance vector routing", Wireless Communications and Mobile Computing, 2006; 6:969–988, © 2006 John Wiley & Sons, Ltd.

[17]. Miss Morli Pandya, Associate Prof. Ashish Kr. Shrivastava (2013), "Review on security issues of AODV routing protocol for MANETs" (M. Tech Scholar, Dept. of Computer Science Engineering, NIIST, Bhopal, India, Oct. 2013.

[18]. Ms. Neetu Singh Chouhan, Ms. Shweta Yadav (2012), "Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering (IJCTEE) publication. Volume 1, Issue 3, 2012

[24]. Ranu Patel, (2013), "Analysis of flooding attack using random waypoint mobility model in mobile adhoc network in NS-3", Elixir Comp. Sci. & Engg, 56A (2013) 13534-13538, 2013 Elixir.

[25]. Ranu Patel, (2013), "Analysis of flooding attack using random waypoint mobility model in mobile adhoc network in NS-3", Elixir Comp. Sci. & Engg, 56A (2013) 13534-13538, © 2013 Elixir.

[26]. Ruchita Meher, Seema Ladhe (2014), "Review Paper on Flooding Attack in MANET" Computer engineering, MGMCET kamothe Navi Mumbai, India January 2014.

[27]. Saba Siraj, (2012), "Network Simulation Tools Survey" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012.

[28]. Sachin Lalar (2014), "Security in MANET: Vulnerabilities, Attacks & Solutions" Department of Computer Science & Engg., TERI, Kurukshetra January 2014.

[29]. SAHAR NAMVARASL, MARZIEH AHMADZADEHA (2014), "Dynamic Flooding Attack Detection System Based on Different Classification Techniques and Using SNMP MIB Data", IJCNCS Publication VOL. 2, NO.9, SEPTEMBER 2014.

[30]. Shani Makwana and KrunalVaghela (2015), "Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET", International Journal of Computer Applications (IJCA) publication. Volume 125 – No.4, September 2015.

[31]. Shikha Jindal, Raman Maini (2014), "An Efficient Technique for Detection of Flooding and Jamming Attacks in Wireless Sensor Networks", IJCA publication. Volume 98– No.10, July 2014.

[33]. ShrutiBhalodiya, KrunalVaghela (2015), "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol", International Journal of Computer Applications (IJCA) publication. Volume 125 – No.4, September 2015.