Engineering Universe for Scientific Research and Management
(International Journal)
ISSN(ONLINE) : 2319-3069
Vol. 7 Issue 3
March 2015

A Novel Approach against RREQ Flooding Grounded on Fuzzy Rule Base

Mahima Trivedi[1], Er. Pawan Patidar[2], Dr. M. K. Rawat[3]
Research Scholar, LNCT, Indore[1]
Asst. Prof., LNCT, Indore[2]
Head of the Dept(CS), LNCT, Indore[3]
trivedimahima.cs@gmail.com[1], pawan.patidar1@live.com[2], drmkrawat@gmail.com[3]

Abstract:- **A Mobile Ad hoc Network is an effortless target of different Security attacks. It' is a network with uncertain infrastructure, ad hoc topology and mobile nodes. This makes it at high risk of being attacked by different security threats. Denial of Service (DOS) has been a major field of research in which RREQ (route request) flooding attack is one of the most common yet serious attacks that targets the AODV protocol, disturbs the routing and eats up the network resources. This manuscript talks about RREQ DOS flooding attack and presents a Novel approach based on Fuzzy Rule Base. The result outcomes illustrated here clearly present the positive effects of the approach.**

Keywords: AODV, DDoS, MANET, RREQ, Fuzzy rule base.

I. INTRODUCTION:

MANET is a network without any fixed infrastructure which means no centralized authority participates in the communication. It is a collection of mobile nodes which communicate with each other via radio waves. Direct communication can occur between nodes that are falling into those radio ranges. Communication beyond these ranges can be completed with the help of intermediate nodes. This phenomenon brings the characteristics of multi hop routing. Due to this very short range of individual entity

the overall performance and efficiency of the network depends upon the number of devices which gradually decreases when the number of nodes increases. Other characteristics provided by MANET such as distributed operation, dynamic topology, lightweight terminals, shared physical medium etc makes it vulnerable to different security attacks. Cooperativeness of nodes and lack of any predefined boundaries, makes MANET a very easy to disturb and prone to various attacks at different layers. Some examples of common attacks are Denial of Service (DOS), wormhole, black hole etc. Here, primary emphasis will be drawn on routing attacks. Starting the discussion about routing in mobile ad hoc networks, in MANET also routing protocols are used for routing packets. Routing in mobile ad hoc network can be broadly divided into two categories reactive and proactive routing. In proactive routing protocols each node in the network makes a routing table and periodically maintenance it. So, whenever the topology changes, it immediately gets reflected in the routing table. This way it also called as table driven routing example. This kind of routing provides minimal delay i.e. a node will immediately get its route but there are some major drawbacks too. Proactive routing protocol consumes network resources even when no node has some data to send. This is because of frequent maintenance of the topology.

On the other hand Reactive routing protocols are different in the way that a node looks for a route only when it needs to communicate with some other node. It uses route discovery procedure to discover routes. For this the initializing node forwards route request(RREQ) packets to its neighbors if it has the destination route it sends back the desired route in the form of route reply(RREP) messages otherwise the node forwards the request its next

neighbor. In this way the request reaches the destination the reply is sent back to the initiative. In this whole procedure each node is considered trustworthy and authentic. This property enables intruders to exploit the route discovery process and consume network resources at results in a very serious kind of attack i.e. flooding attack. A flooding attack occurs when the intruder sends certain packets repeatedly. In this manuscript, a novel approach based on fuzzy rule base is going to be presented which will work for RREQ flooding attack occurred in reactive routing protocols such as AODV.

This paper is organized as follows
Section 2 describes the working of a AODV protocol.
Section 3 will provide details about flooding attack.
Section 4 will tell about related works in this field.
And then Section 5 will discuss the proposed approach.

II. AODV:

AODV(Ad hoc On demand Distance Vector) being a reactive routing protocol uses route discovery method as discussed in previous section for discovering new routes. The protocol uses flooding method and sends RREQ packets to its neighbors. If the neighbor does not have the requested route, it again sends the RREQ to its next neighbors. This route discovery process is also known as expanding ring method. After receiving the request, any node having routes, replies with RREP message and sends valid routes. AODV is a MANET routing protocol. Mutual trust and authenticity of node is considered by default. Means it is considered that each node in the network sends valid requests. With this fact, it becomes very easy for any intruder to attack the network using the AODV protocol. Upcoming section will discuss about the most common DDOS (Distributed Denial of Service) attack i.e. flooding attack with affects the network resources and routing table and the result is totally disrupted routing and packet loss.

III. RREQ FLOODING ATTACK:

As mentioned in previous section RREQ flooding attack is a type of flooding or DDOS/DOS attack. Let's first understand what DOS attack is. Denial of service attack is actually a bunch of attacks whose aim is to make certain service unavailable and the victim less efficient. This can be done either by force stop or by consuming too many resources to make it disable towards responding valid request. This attack uses the latter approach and makes nodes so busy that they cannot process genuine request. Soon the victim nodes get out of resources because of limited bandwidth and power. The only difference between a DOS and DDOS attack that the DDOS attack has multiple attacking nodes. There are different DOS attacks targeting different layers of communication, such as RREQ flooding, hello packet flooding, SYN flooding, jamming attack etc.

RREQ flooding attack being a DDOS attack targets the resources of network and affects the overall routing. In this attack the malicious nodes repeatedly send packets to find a route for a node that does not exist in the network. In this way the attacker eats up the routing table and data packets get lost due to presence of invalid routes in the routing table. AODV and other reactive routing protocols proposed for MANET can easily be affected by this because in such protocols the route discovery works by flooding RREQ control packets in the network. This flooding or blind flooding increases control overhead. Ad hoc networks contain limited bandwidth and limited energy can easily get congested by these attacks. Therefore with increase of load and mobility of nodes the control packets can consume more and more bandwidth of the network. This characteristic works as an inspiration for malicious nodes and they generate flood of false control packets. Because of the highest priority of control packets the transmission of RREQ packets will dominate even at the high loads which will result in wastage of energy, disrupted routing mechanism and low packet delivery ratio. As consequences little or no valid communication can occur in the network and finally it will be a denial of service.
The RREQ flooding affects the network so badly that even a single attacker node can degrade the performance 84-

90%. With increase of attacker node, packet delivery ratio and overall throughput falls down. Table1 shows the impact of RREQ flooding on the network.

No. of Attackers	Packet Loss	Throughput (Bytes)	Delay
None	3.5%	8255	0.59
1	54%	2324	9.6
2	75%	1287	10
3	>82%	589	10

IV. Related Work:

Flooding attack can adversely affect network performance by draining battery and computation power as well as the bandwidth of the network. It can be of different types depending upon the layer, for example RREQ flooding [6] attack is triggered on the network layer, and SYN flooding [7] attacks on transport layer. With this change, the underlying protocols change from layer to layer. Let us now discuss different prevention mechanisms introduced so far. A self organized public key management was introduced in [8], for supporting routing protocols of MANET. [9] Discussed another approach which was based on cryptography. They presented a mechanism for distributing certificate authority (CA) public key. By doing this they tried to form a collective CA service. Apart from these cryptographic approaches, some traffic based approaches has also been deployed. Neighbor suppression method [10], in which each node monitors and calculates the rate of its neighbor node's RREQ. If it exceeds the predefined threshold, the node is blacklisted. Another adaptive technique was presented in [11], which is based on statistical analysis for detecting RREQ floods. Flooding attack prevention (FAP) [12] was method tested on AODV routing protocol. Adaptive intrusion detection technique [13] uses anomaly based intrusion detection as its grounds. It works in two phases, training phase and testing phase. Normal behavior of the network is recorded in training phase and any fluctuation or change is detected in the testing phase by comparison. A trust based prevention mechanism was presented in [14] and [15]. In this technique, they introduced three filtering criteria to mark three node relationships i.e. friend, acquaintances and stranger. They included the concept of delay queue to handle nodes with higher mobility. Along with these filtering based techniques, there is also, capability based approach [16], to handle flooding attacks on transport layer. These methods are based on the principle "Deny by Default". In this technique, each node is assigned a capability which is a special token. This capability is issued by the responder of any transport layer flow to initiator, to urge a limit on the amount of traffic that can be sent through the flow within a certain period of time. When it comes to a monitoring based approach, it becomes easy and proves proper justification to participating nodes. Now the question that arises is what to monitor? So far, techniques based on monitoring and filtering have been introduced. The research presented in this paper is using the same approach with monitoring of three parameters i.e PDR, Change in Energy and Average no. of packets.

Malicious attackers and intruders in MANET are using concealed identity with the practice of IP Spoofing and other techniques. To overcome this issue Jin, Xin, et al. [16] presented a novel approach based on zone sampling and adds up a "Zone_ID". Next, a path is reconstructed. But, these trace back kind of methods do not result good in dynamic scenarios. Furthermore there are some other counter techniques based on clusters, such as a cooperative technique suggested by Yian
Huang and Wenke Lee [17] in which an ID agent is elected for each cluster and detection is done based on training data of preceptors used. But, it fails when we do not have linear separable points. In some more efforts based on Fuzzy logic for example in [19] by S. Ahmed and S. M. Nirkhi in which log files are traced to provide a forensic analysis approach via tracking RREP messages. However, the ground of their research was DSR which fails in a heavy load traffic network. For implementation

they used .Net framework. These types of approaches may work slow because of complex working and a slow working platforms.

The Table presented below, compares previous fuzzy based approach with the proposed approach:

	Previous Technique	Proposed Technique
Approach Used	Investigation After Attack Occurred	Prevention Before Attack Occurs
Platform Used	.Net	NS2
Parameters Used	Total RREQ, Hop Count. Total RREP, Message Length, Time duration.	PDR, Residual Energy and Avg. Requests
Routing Protocol	DSR	AODV

First and foremost drawback of the previous approach was that it activates after the attack occurred in the network and then investigates the network. The proposed approach activates within a few milliseconds of the simulation and then prevents attacker node to affect the network badly. Use of a number of parameters and reading of logs, potentially makes the previous approach slow. Also, the protocol used was DSR which indeed fails in heavy load traffics. In the proposed approach, on the other hand AODV is used which is a better choice over DSR.

V. PROPOSED APPROACH

Flooding or DoS attack, as already discussed greatly affects the performance of a network, even with a single attacker node, it can degrade the performance of a network enormously. Let us now discuss and muse over the proposed approach to counter the attack which is discussed above. Proposed algorithm takes into consideration three parameters which are PDR, Change in Energy and Average no. of packets sent by a node. Then after, a fuzzy rule base is prepared. As mentioned in the previous section, a fuzzy based approach gives you more flexibility to solve a problem. In this scenario, a number of combinations of these three are monitored and a fuzzy rule base is prepared, which yields proper justification to all the participating nodes. Different combinations of the parameters are assigned different threshold values, called as trust factor. Node trust factor less than the threshold will not be entertained and nodes having above or equal to the threshold will be while listed. Below section will discuss role of all the parameters in the proposed approach.

5.1 Fuzzy Rule base

Basically, fuzzy logic [5] is a multi-valued logic that enables transitional values to be classified between conventional yes/no like evaluations. Examples of fuzzy based notions will be rather warm or pretty cold which can be formulated mathematically and algorithmically. Fuzzy logic systems target the approximation and ambiguity of input and output variables by defining fuzzy numbers and fuzzy sets that can be expressed in linguistic variables. Fuzzy rule-based approach to modeling is based on verbally formulated rules overlapped throughout the parameter space. They use numerical interpolation to handle complex non-linear relationships. A linguistic fuzzy rule is just an “If Then construct” that can be expressed in following way:

If X is A

Then Y is B

5.2 PDR:

An attacking node will have a low packet delivery ratio (PDR) as it sends fake RREQ packets. By monitoring this parameter one can track an attacker node. A low PDR of a node shows high probability of being attacker node. In this

rule base, High (H) in PDR means low value of a node's PDR and high probability of being a malicious node.

5.3 Change in Energy (Residual energy)

In Manet, nodes have limited battery power and limited computation energy. Nodes having fast draining energy or a big change in energy may be a malicious node as it floods large number of fake RREQ packets in the network. In the rule base, energy with High attribute means high change in energy that clearly means high probability of being a malicious node.

TRUST FACTOR	ENERGY RESIDUAL	PDR	AVG. REQUESTS
-5	**H**	**H**	**H**
-1	H	H	L
-3	H	L	H
-5	L	H	H
0	M	M	M
1	M	M	L
1	M	L	M
0	L	M	M
1	**L**	**L**	**L**
-1	L	L	H
0	L	H	L
0	H	L	L
-1	H	H	M
-1	H	M	H
-1	M	H	H
0	L	L	M
0	L	M	L
0	M	L	L

5.4 Average Number of Packets

Counting on an average number of packets is a vital factor in a filtering based approach. Average of the packets a node is sending in the duration is very important. A malicious node will have a high number of packets sent. In proposed rule base High of this attribute means high probability of being a malicious node.

5.5 *The Rule Base*

The rule base of proposed solution is designed on three attributes that are PDR, Change in Energy and average number of packets. Combinations of different linguistic rules corresponding to Low (L), medium (M) and high (H) levels of the attributes have been used here. High on residual energy shows that the node contains low energy which is a harmful condition. High on PDR means node contains low PDR, means high probability of attacker node. High of RREQ packets means sending more packets and high likelihood of being attacking node. Next, on the basis of these linguistic rules, a "Trust Value" is assigned that varies between -5 to +1 depending upon the possibility of attacker node. For a High in all the attribute which is the most certain odd of being a damaging node is assigned a value of -5 and for a Low in all means the node is normal and there is least chance of being an attacker. Different combinations of these linguistic rules have assigned different trust values. A negative magnitude of truth value means the node may be a attacker and should be blacklisted. Any request packet from a blacklisted node will be ignored and no processing will be performed. This way effect of RREQ flooding can be minimized.

VI. Proposed Algorithm

In the DDos attack the main purpose of the attacker node is to drain the energy of the network nodes and the use all the available bandwidth so the original request are packets were not send .In proposed algorithm different rules have to be made in terms of energy, PDR, Average Requests/sec and the risk factor of nodes in terms of H , M ,L and assign values to them. Finding an attacker node follows the following steps:

Step 1: Compute the remaining energy of the all nodes.
Step 2: Compute the Packet Delivery Ratio of each nodes.

Step 3: Find out the Request sent by the node per second.

After finding the values , of energy, PDR, average requests/sec Calculate the weight of the each node and than using Rule based method assign values (HIGH ,MEDIEM ,LOW) to the nodes and assign numeric weight as (0 ,-1 ,1 ,5 ,-5) chance of attacker if any nodes having weight less than fixed threshold, than set as attacker and stop receiving request of these nodes for fixed time and then after every fixed time interval repeat the process for getting new values and then again assigning weight to all the nodes and compare again with threshold.

VII. Result Outcome:

Figures shown below depict the simulation results of the work. It clearly demonstrates the effect of flooding attack on the network in terms of overall routing overhead and change of energy of nodes. Simulation of 30 seconds has been taken, when the scenario is normal; there is less fluctuation in energy and when it is under attack, energy drops down so fast. Result after applying the proposed algorithm, the drain of energy is totally under control. Similarly, the second figure shows us the average number of requests per second. Under attack, there is high amount of requests in one second, and after applying the solution, it is not much high. Similarly, the Packet Delivery Ratio (PDR) is also improved which was degraded to around 20% of the actual PDR. Figure 1 here shows a reduced consumption of energy after the prevention algorithm applied into the simulated network. Subsequently, Figure 2 and 3 displays improved Routing overhead and PDR.

VIII. Conclusion and Future Work

RREQ flooding attack is one of the most serious DDOS attacks that targets network discovery phase of routing. This manuscript presented a solution based on fuzzy rule base and demonstrated the result outcomes. Results presented here clearly demonstrate the performance in terms of Energy, PDR and Routing overhead. If the graphs are studied carefully, it will show that more than 4o% of enhancement has been achieved by applying the algorithm. Future enhancement of this approach may include some other parameters. Also, it can be implemented for other kind of flooding attacks with minor modifications.

References

[1]. Praveen Joshi, "Security issues in routing protocols in manet at networ klayer" Elsvier 2011.

[2]. Sharma, Kuldeep, and Neha Khandelwal. "Prabhakar. M,“An Overview Of security Problems in MANET”." Proceedings of the International Conference on Network Protocols (ICNP). 2010.

[3]. Praveen Joshi, "Security issues in routing protocols in manet at network layer" Elsvier 2011

[4]. Perkins eg. al. "Adhoc on demand distance vector (AODV) Routing", July2003.

[5]. Bhuvaneshwari K. , Dr. A Francis saviour devraj,"Examination on impact of flooding attack on manet and to accentuate on performance degradation" Int. J Advanced networking and Apps. 2013

[6]. Wang, Haining, Danlu Zhang, and Kang G. Shin. "Detecting SYN flooding attacks." INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 3. IEEE, 2002.

[7]. Sahadevaiah, K., and O. B. V. Ramanaiah. "Self-Organized Public Key Cryptography in Mobile Ad Hoc Networks." Journal of Ubiquitous Computing and Communication.

[8]. Mohd. A. Alhabeeb,Abdullah Almuhaideb and phu dung le," Holistic approach for critical system security:flooding prev. And mal. Packet stopping" Journal of telecomm. Vol I Issue 1 ,2010.

[9]. Yi, Ping, et al. "A new routing attack in mobile ad hoc networks." International Journal of Information Technology 11.2 (2005): 83-94.

[10]. Song, Jian-Hua, Fan Hong, and Yu Zhang. "Effective filtering scheme against RREQ

flooding attack in mobile ad hoc networks." Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies. IEEE Computer Society, 2006.

[11]. Samam Desilva, Rajendra V. Boppan,"Mitigating malicious control packet floods in Ad hoc Networks", IEEE wireless communications and networking conference, March 2005.

[12]. Adnan Nadeem, Michael howarth," Adaptive intrusion detection and prevention of denial of service attacks in MANETS" ACM 2009

[13]. Shishir K. Shandilya, Sunita Sahu ,"A trust based security scheme fir RREQ flooding attack in MANET" International journal of computer applications aug 2010.

[14]. Ujwala D. Khartad and R. K. Krishna,"Route request flooding attack using trust based security scheme in manet", International journal of smart sensors and Ad hoc Networks (IJSSAN), 2014.

[15]. Jia, Quan, Kun Sun, and Angelos Stavrou. "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET." Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on. IEEE, 2011.

[16]. Jin, Xin, et al. "ZSBT: A novel algorithm for tracing DoS attackers in MANETs." EURASIP Journal on Wireless Communications and Networking 2006.2 (2006): 82-82.

[17]. Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM, 2003.

[18]. Ahmed, Ms Sarah, and Ms SM Nirkhi. "A Fuzzy Rule Based Forensic Analysis of DDoS Attack in MANET." International Journal of Advanced Computer Science and Applications (IJACSA) 4.6 (2013).

IX. List of Figures

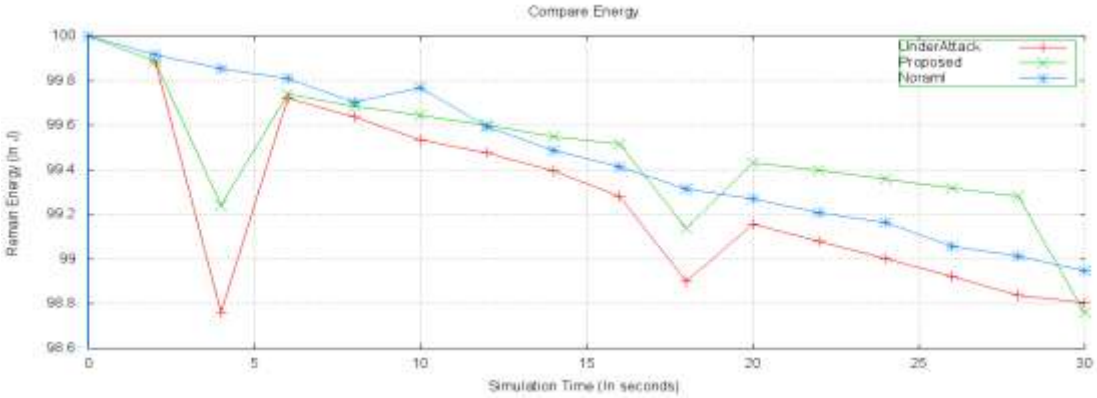

Figure 1: Energy Comparison

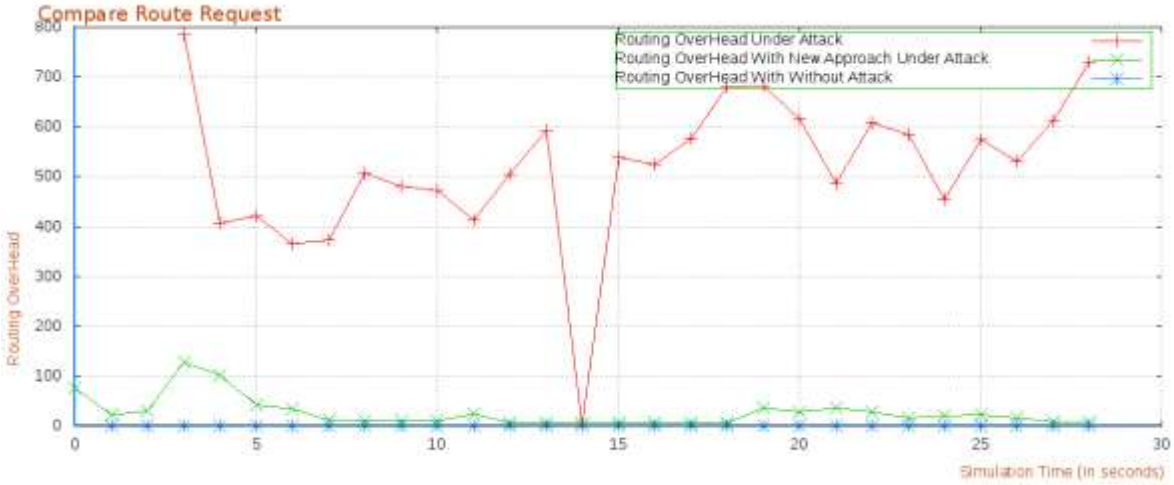

Figure 2: Routing Overhead Comparison

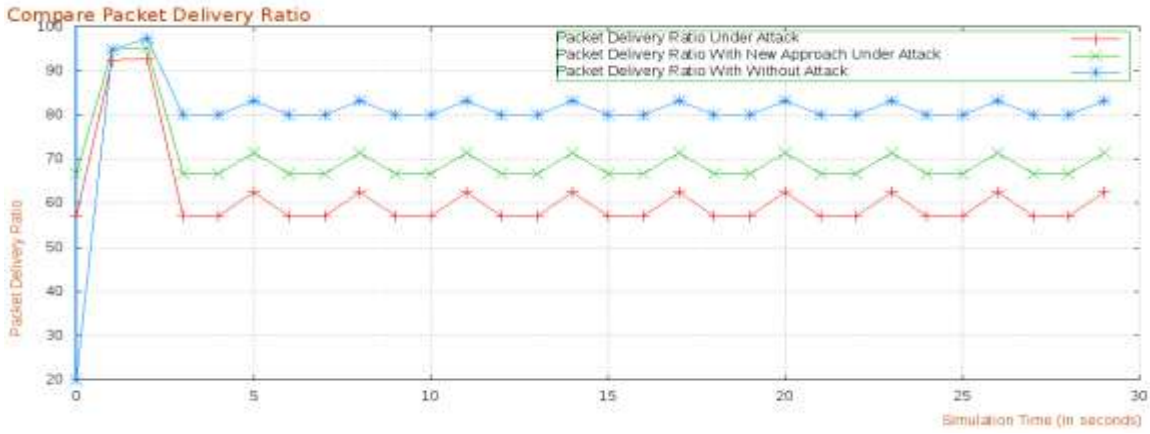

Figure 3: PDR Comparison