iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 2 **Issue:** IV **Month of publication:** April 2014

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

# Mitigation of flooding Attack in MANET using NS-3

Abhijeet kumar 1, Archana Bharti 2

*1 (Electronics and Communication Engineering )*
*College of Engineering Science and Technology,*
*Lucknow, Uttar Pradesh, India*

*2 (Mechanical Engineering)*
*Sanjay Gandhi Polytechnic*
*Jagdish pur (U.P) , India*

***Abstract: Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. A simulation study of the effects of flooding attack on the performance of the AODV routing protocol is presented using random waypoint mobility model .The simulation environment is implemented by using the NS-3 network simulator. It is observed that due to the presence of such malicious nodes, average percentage of packet loss in the network, average routing overhead and average bandwidth requirement− all increases, thus degrading the performance of MANET significantly.***

***Keywords - MANET, flooding attack, Denial of Service (DOS), packets, route request.***

## 1. INTRODUCTION

Mobile Ad-hoc Network (MANET) refers to a form of infrastructure less network connecting mobile devices with wireless communication capability. Each node behaves as a router as well as an end host, so that the connection between any two nodes is a multi-hop path supported by other nodes [1].

MANET represents a system of wireless mobile nodes that can freely and dynamically self-organize in to arbitrary and temporary network topologies, allowing people and devices to communicate without any pre-existing communication architecture. Each node in the network also acts as a router, forwarding data packets for other nodes.

They communicate directly with devices inside their radio range in a peer-to-peer nature. If they wish to communicate with a device outside their range, they can use an intermediate device or devices within their radio range to relay or forward communications to the device outside their range. An ad hoc network is self-organizing and adaptive [2].

MANET are generally formed for short range communication. The performance of the network depends on the number of devices; it degrades as the number of device increases because all the devices shares the available network resources. Like conventional wired network MANET also uses routing protocols to route the packets to its destination.

Ad hoc networks routing protocols are divided into two categories: Proactive and reactive [3].

Proactive routing protocols are also known as “table driven” routing .In this, all the nodes store the routing information about other node present in the networks and routing updates are propagated in the network whenever network topology changes.

The advantage of proactive routing protocol is that node experiences minimal delay when route is needed and unexpired route is available in the routing table but the disadvantage of proactive routing is that these are not scalable and maintenance of routing table requires substantial network resources.

In the case of reactive routing protocol, route between the nodes is searched only when node wants to communicate with other node. To discover the routes they use route discovery procedure which in turns uses the flooding method. In this, initiator forwards the RREQ packet to all of its neighbour’s.

If neighbour has the route for destination they reply otherwise forward the RREQ to the next node. In this way RREQ packet reaches to the destination which sends the reply to RREQ. But the method which is used to facilitate route discovery are used by the Intruders or the malicious node to consume the network resources which may lead to flooding attack.

## 2. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING (AODV)

In order to bring computation to environments and with a minimal infrastructure, Ad Hoc Networks are quite helpful.[4][5][6]

Mobile Ad-hoc networks are composed of autonomous wireless nodes i.e. it requires no central node to manage the networks.

All the work is done with the mutual agreement and understanding between the nodes.

Thus every node will work in both configurations:

1. "As a router"
2. "As a host"

On account of mobility nature of nodes, topology of the network changes with time and makes the ad-hoc network to be a non–infrastructure network. Every node has the self-configuring ability.

This results to Security problems are there in mobile ad hoc network.Every Node has the responsibility of forwarding the packets received by it. But due to lack of security mechanism in routing protocols, nodes can behave unexpectedly and absorbs the packets without forwarding it.There are various types of Dos attacks that can occur in such a network, so it is essential to detect such kind of attack and methods to exclude the malicious or misbehaving nodes and enhance the nodes cooperation.

REQ Flooding & DoS Effect

The default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. In AODV, a malicious code can override the restriction put by the RREQ_RATELIMIT, either by increasing it or disabling it.

A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a very high number. This results to DoS attack on the networks flooded by fake RREQs and problems as follows:

1. Bandwidth wastage.
2. Increase in Routing Overhead.
3. Traffic in entries of Routing Table.
4. Battery Power Wastage.
5. Degradation in Throughput.

(NOTE: Compromised node is the internal node which behaves maliciously which results in Fake RREQ Flooding.)

Combat the DoS Effect

As mentioned earlier, the default value for RREQ_RATELIMIT is 10 RREQs/sec. This means each node is expected to observe some self-control on the number of RREQs it sends in one sec. A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a very high number or even disable this limiting feature, thus allowing it .Thus allowing it to send large number of RREQ packets per second.

The proposed scheme shifts the responsibility to monitor this parameter on the node's neighbor, thus ensuring the compliance of this restriction. This solves all of the problems caused due to flooding of RREQs from a compromised node. Thus instead of self-control, the control exercised by a node's neighbor results in preventing the flooding of RREQs.

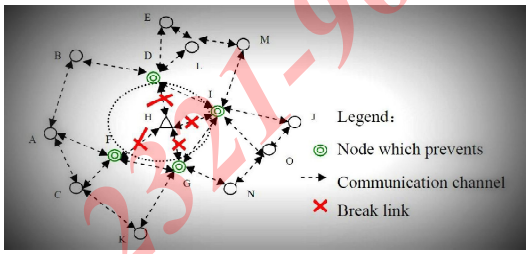



Figure 1 : AODV

Parameters involved in Combat

RREQ_ACCEPT_LIMIT: This specifies a value that ensures uniform usage of a node's resources by its neighbors. RREQs exceeding this limit are dropped, but their time stamps are recorded. This information will aid in monitoring the neighbor's activities. In the simulations carried out, the value of this parameter was kept as three (i.e. three RREQs can be accepted per unit time). This value can be made adaptive, depending upon node metrics such as it memory, processing power, battery, etc.

RREQ_BLACKLIST_LIMIT : This specifies a value that aids in determining whether a node is acting malicious or not. To do so, the number of RREQs originated/forwarded by a neighboring node per unit time is tracked.

If this count exceeds the value of RREQ_BLACKLIST_LIMIT, one can safely assume that the corresponding neighboring node is trying to flood the network with possibly fake RREQs. On identifying a neighboring node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network.

BLACKLIST_TIMEOUT: The period of time the blacklisted node is ignored after which it is unblocked. Thus period is doubled each time the node repeats its malicious behavior.

In the simulations the value of RREQ_BLACKLIST_LIMIT is kept as 10 (i.e. more than 10 RREQs per unit time results in flooding activity). By blacklisting a malicious node, all neighbors of the malicious node restrict the RREQ flooding. Also the malicious node is isolated due to this distributed defense and so cannot hog its

neighbor's resources. The neighboring nodes are therefore free to entertain the RREQs from other genuine nodes. Nodes that are confident about the malicious nature of a particular node, can avoid using it for subsequent network functions. In this way genuine nodes are saved from experiencing the DoS attack.

## 3. NETWORK SIMULATOR-3

The Ns-3 Simulator For simulation analysis NS-3 [7] [8] was used for implementing the network simulation environment. NS-3 is an open source discrete event network simulator targeted primarily for networking research and educational purpose. Previously, NS-2 [9] was the tool for academic networking research. But it had several disadvantages. It required the involvement of both oTcl and C++.

For new modules and features, it required a lot of manual recoding and compilations. NS-3 is a new simulator. It is not an extension of NS-2. It does not support the NS-2 APIs. It is written entirely in C++, with optional Python bindings. Hence simulation scripts can be written either in C++ or in Python. The oTcl scripts are no longer needed for controlling the simulation thus abandoning the problems which were introduced by the combination of C++ and oTcl in NS-2.

Thus, NS-3 is a more readily extensible platform and much easier to use.NS-3 has sophisticated simulation features, which include extensive parameterization system and configurable embedded tracing system, with standard outputs to text logs or PCAP (tcpdump). It is very object oriented for rapid coding andextension. It has an automatic memory management capability as well as an efficient object aggregation/query for new behaviors & states, like adding mobility models to nodes. Moreover, NS-3 has new capabilities, such as handling multiple interfaces on nodes correctly, efficient use of IP addressing and more alignment with Internet protocols and designs and more detailed 802.11 models, etc. NS-3 integrates the architectural concepts and code from GTNetS [10], which is a simulator with good scalability characteristics.

The Simulation Network Architecture looks just like IP architecture stack. The nodes in NS-3 may or may not have mobility. The nodes have "network devices", which transfer packets over channel and incorporates Layer 1 (Physical Layer) & Layer 2 (Data Link layer). The network devices acts as an interface with Layer 3 (Network Layer: IP, ARP). The Layer 3 supports the Layer 4 (Transport Layer: UDP, TCP), which is used by the Layer 5 (Application Layer) objects.

## 4. LITERATURE SURVEY

Author Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury [16] have suggested default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. However, a malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node is able to do so because of its self-control over its parameters. This permits it to flood the network with false route requests, leading to a type of DoS attack due to the network-load forced by the false RREQs.

Author Humaira Ehsan and Farrukh Aslam Khan [17] has been suggested evaluation of network performance for AODV especially in terms of packet efficiency, routing overhead, and throughput.

Author Arpita Raverkar [18] has been define three parameter Route discovery, throughput and delay for detection of flooding attack.

Author S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam [19] has been used to detect malicious node who floods in the network using RREQ messages, has proposed a statistical approach to avoid the forwarding of such packets via the concept of RREQ counts.

Author Abdur Rashid Sangi, Jianwei Liu and Likun Zou [20] has been discuss about attack has been done by the authorize node. Attacks have been initiated by authenticated nodes/devices in Ad Hoc Network to disrupt the network called byzantine attack. Although these attacks can be initiated independently but are more distressing if start in a mutual way. They highlight the performance degradation of AODV routing protocol, when the byzantine attack are initiated in a combination.

## 5. SIMULATION SETUP

The metrics in the Network Simulation are the important factors of network performance, which have been used to compare the performance of the proposed scheme in the network with the performance of the original protocol.

1) End-to-End Delay: Average time difference (in seconds) between the time of the packet receipt at the destination node, and the packet sending time at the source node.

2) Round Trip Time (RTT): Time difference between the receipt of the acknowledgement from the destination node to the source node, and the time of sending of the original packet at the source node.

3) Average simulation processing time at nodes for a packet: Time difference between the packet forwarding time and the packet receipt time at a given node.

4) Average number of nodes receiving packets: Sum of numbers of all the intermediate nodes (nodes between source and destination nodes) receiving packets sent by all the source nodes / number of received packets at all the destination nodes.

5) Average number of nodes forwarding packets: Sum of numbers of all the intermediate nodes (nodes between source

and destination nodes) forwarding packets sent by all the source nodes / number of received packets at all the destination nodes.

6) Delays between current and other node: Shows end-to-end delays (in seconds) between current node (sender) and other node (receiver).

7) Number of data packets dropped: The number of data packets dropped at any given node. This is an important parameter because if the number of dropped packets increases, the throughput would decrease.

8) Throughput: 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.

NS- 3 simulation set Up for Wireless network

| PARAMETERS | VALUES |
|---|---|
| Routing Protocol | AODV |
| Simulation Time | 60s |
| No of mobile Nodes | 95 |
| Transmission Area | 1000 x 1000 |
| Mobility Model | Random- walk 2D |
| Traffic Type | UDP |
| Data Packet Size | 1Kb |
| Rate | 2kb/s |
| Speed Of Node | 20 m/s |
| Proposed RREQ_RATELIMIT | 10 |

PROPOSED SCHEME :

AIM:

"Control the spread of RREQ packets and reduce the effects of broadcast attacks using RREQ."

ASSUMPTION:

"We assume that there exists a security mechanism, such as public key cryptography and digital signatures or MAC (Message Authentication Code) that enables a node to authenticate routing messages from any node in the network."

Therefore, a malicious node cannot spoof the originator and destination IP addresses in a RREQ packet although the destination IP address may not be reachable in the network.[11][14][15]

DESCRIPTION

- The proposed technique uses a filter to detect misbehaving nodes and reduces their impact on network performance.
- The aim of the filter is to limit the rate of RREQ packets.
- Each node maintains two threshold values.
- The threshold values are the criterion for each node's decision of how to react to a RREQ message.
- The RATE_LIMIT 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 RATE_LIMIT, the RREQ packet is processed as normal.
- The BLACKLIST_LIMIT parameter is used to specify 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 BLACKLIST_LIMIT, 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 given by BLACKLIST_TIMEOUT after which it is unblocked. The proposed scheme has the ability to block a node till BLACKLIST_TIMEOUT period on an incremental basis.
- By blacklisting a malicious node, all neighbors of the malicious node restrict the RREQ flooding.
- Also the malicious node is isolated due to this distributed defense and so cannot hog its neighbor's resources.
- 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.
- If the rate of RREQs originated by a node is between the RATE_LIMIT and the BLACKLIST_LIMIT, the RREQ packet is added to a "delay queue" waiting to be processed.
- Every time a DELAY_TIMEOUT expires, if there is anything in the delay queue (RREQ packet waiting to be processed), then the first packet is removed to be processed.
- To do so, malicious node that has a high attack rate will thus be severely delayed.
- Meanwhile, the proposed rate control mechanism will have no impact on other nodes and also have

minimal impact on the normal nodes that send abnormally high RREQs.

- The filtering forwarding scheme slows down the spread of excessive RREQs originated by a node per unit time and successfully prevents DoS attacks.
- The proposed scheme incurs no extra overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV. Also the proposed scheme is more efficient in terms of resource reservations and its computational complexity. In addition to limiting the clogging up of resources in the network, the proposed scheme also isolates the malicious node.

Algorithm for RREQ Flooding Attack
TVL –> THRESHOLD_VALUE_LIMIT
TVL cl ose neig hbor –> Threshold Value of Closest Neighbor (MOST TRUSTED)
TVL neighbor –> Threshold Value of nearby Neighbor (TRUSTED)
RAL –> RREQ_ACCEPT_LIMIT
RBL –> RREQ_BLACKLIST_LIMIT
RRL –> RREQ_RATE Broadcasted
TTL –> Time To Live
DR –> Data Rate
nR –> Number of Retries

1. STATE : : Begin
2. Receive an RREQ.
3. CHECK_NODE (TVL){
4. If

4.1 CONDITION : : TVL > = TVL close neighbor => Node :: Close Neighbor
4.2 Call PROCESS_RREQ

5. Else If

5.1 CONDITION : : TVL neighbor < =TVL < TVL Close Neighbor => Node :: Neighbor
5.2 Call PROCESS_RREQ

6. Else If

6.1 CONDITION : : 0 < TVL < T neighbor = > Node :: Unknown
6.2Call PROCESS_RREQ

7. Else

7.1 STATE : : Undefined

8. }
9. PROCESS_RREQ (TTL, DR, nR){

7.1 If
7.1.1 CONDITION : : RRL < RAL
7.1.2 STATE : : Acceptance
7.1.3 Process as Normal
7.2 Else If
7.2.1 CONDITION : : Rate RRL > RBL
7.2.2 Add to Blacklist
7.3 Else If
7.3.1 CONDITION : : RAL < RRL < RBL
7.3.2 Add to Delay Queue.
7.4 Else
7.4.1 STATE : : Termination
10. }
11. Stop

## 6. SIMULATION RESULTS

After simulating the flooding attack in AODV, some graphs were plotted and they were used to see the simulation results when the network gets flooded by fake RREQs to invalid destinations.
From Figure 2,The average Routing Overhead increases with the number of fake RREQs, Due to routing table of each node needs to maintain more entries, thus creating an extra overhead.
From Figure 3 ,The graph indicate that the average percentage of data packet loss increases with the increase of fake RREQs in the network.
From Figure 4, Here increase number of flooding nodes,which generate eight RREQ per sec.
Increase the number of flooding nodes, Routing Overhead, (i.e. total number of original and ake RREQ packets in the network) increased drastically.

Bandwidth usage = (Total number of packets received/Simulation Time)*(8/1000)

Bandwidth usage of a network is inversely proportional to the throughput of the network.

From Figure 5,The average bandwidth usage of the network increases as more flooding nodes join the network. Because of this flooding attack,average bandwidth usage of the network increases considerably, thus decreasing the network throughput

From Figure 6,The average percentage of data packet loss in the network increases with the number of flooding nodes.

From Figure 7,The number of flooding nodes in the network increases, the average packet loss (both data and routing packets) also increases in the network.

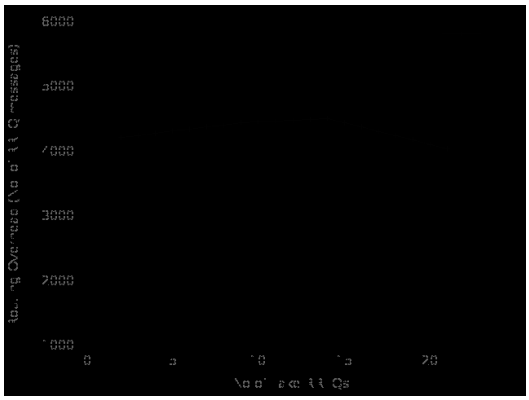


Figure 2 : Number of fake RREQs vs. Routing overhead

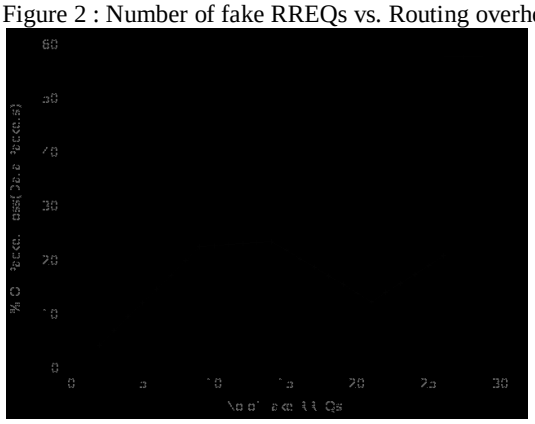


Figure 3 : Number of fake RREQs vs.Percentage of Data Packet Loss

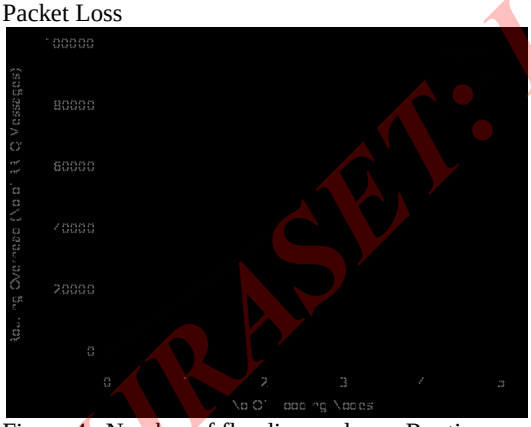


Figure 4 : Number of flooding nodes vs.Routing overhead

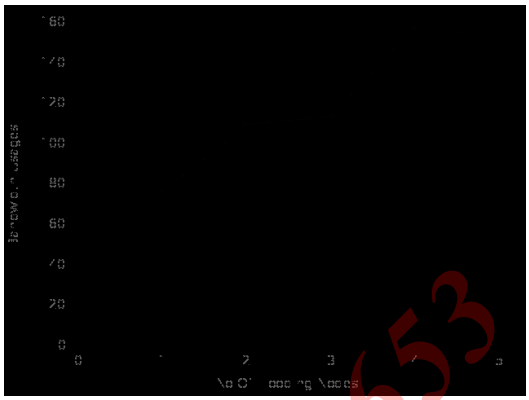


Figure 5 : Number of flooding nodes vs. Bandwidth usages

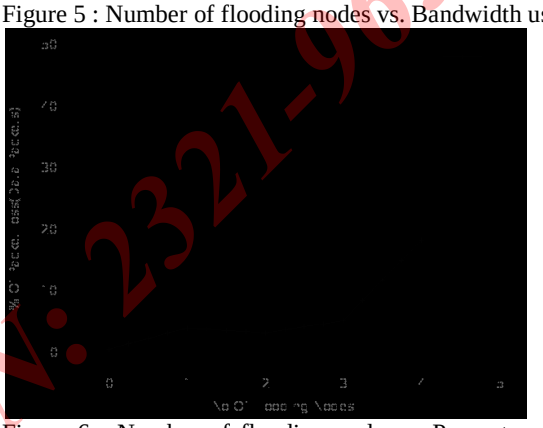


Figure 6 : Number of flooding nodes vs.Percentage of Data Packet Loss

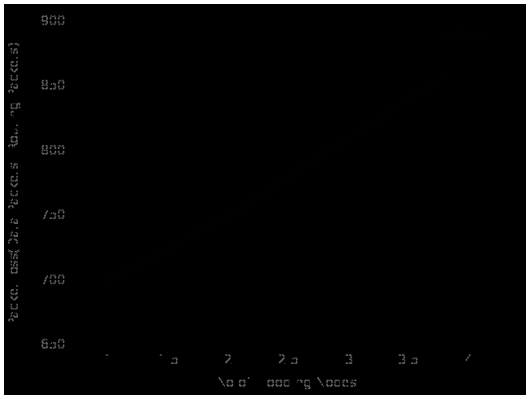


Figure 7.Number of flooding nodes vs.Percentage of overall packet Loss

## 7. CONCLUSION AND FUTURE WORK

We found out how DoS attack was caused on account of RREQ Flooding. Then with the help of proposed scheme, we detected the DoS attack because of RREQ flooding. We also

detected the malicious nodes and blacklisted. In this process none of the genuine nodes which may be wrongly accused of being mischievous were not malicious.

The performance of the network was enhanced in the presence of compromised nodes and making the limit-parameters adaptive in nature.This can be done by making calculations based on parameters like memory, processing capability, battery power, and average number of requests per second in the network and so on. Further, the protocol can be made secure against other types of possible DoS attacks that threaten it.

Mobile computing involves mobile communication. The issues related to this networks are ad hoc and infrastructure networks as well as communication properties, protocols and the like.

Thus the scope of enhancement and improvements in Wireless Networks, preferably Mobile Ad Hoc Networks is enormous.

REFERENCES

[1] M. Gerla, J.T. Tsai, "Multicluster Mobile, Multimedia Radio Network," ACM-Blatzer Wireless Networks, vol. 1, pp. 255-65, 1995.

[2] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Englewood Cliff, Press: Prentice Hall, 2002.

[3] Elizabeth M. Royer, University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology ,"A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" IEEE personal communication, Apr 1999.

[4] Mobile Ad Hoc Networking Working Group, Charles E. Perkins Nokia Research Center,22 October 1999, Elizabeth M.Royer University of California, Santa Barbara Samir R.Ds University of Texas, San Antonio Ad Hoc On-Demand Distance Vector (AODV) Routing.

[5] Krishna Ramachandran. Aodv. Technical report, University of California, Santa Barbara, USA URL: http://moment.cs.ucsb.edu/AODV/aodv

[6] Lee K. Thong. "Performance Analysis of Mobile Adhoc Network Routing Protocols". Thesis Paper submitted to the Department of Computer Science, Naval Post Graduate School, Monterey,CA 2004.

[7] "The NS-3 Network Simulator", http://www.nsnam.org/

[8] Elias Weingartner, Hendrik vom Lehn, Klaus Wehrle, "A performance comparison of recent network simulators". In Proceedings of the IEEE International Conference on Communications 2009 (ICC 2009), Dresden, Germany, 2009.

[9] "The NS-2 Network Simulator", http://www.isi.edu/nsnam/ns

[10] G. Riley, "Large scale network simulations with GTNetS", in Proceedings of the 2003 Winter Simulation Conference, 2003.

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

[12] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hocnetworks", Proc. of Wireless Comm., IEEE, Oct 2007, Issue 5, pgs 85-91.

[13] S. Sanyal, A. Abraham, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N. Mody, "Security scheme for distributed DoS in mobile ad hoc networks", 6th International Workshop on Distributed Computing (IWDC'04), vol. 3326, LNCS, Springer, 2004, pp. 541.

[14] P. Yi, Z. Dai, Y. Zhong, S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), April 2005, pp. 657-662.

[15] Z. Eu and W. Seah, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan, January 2006

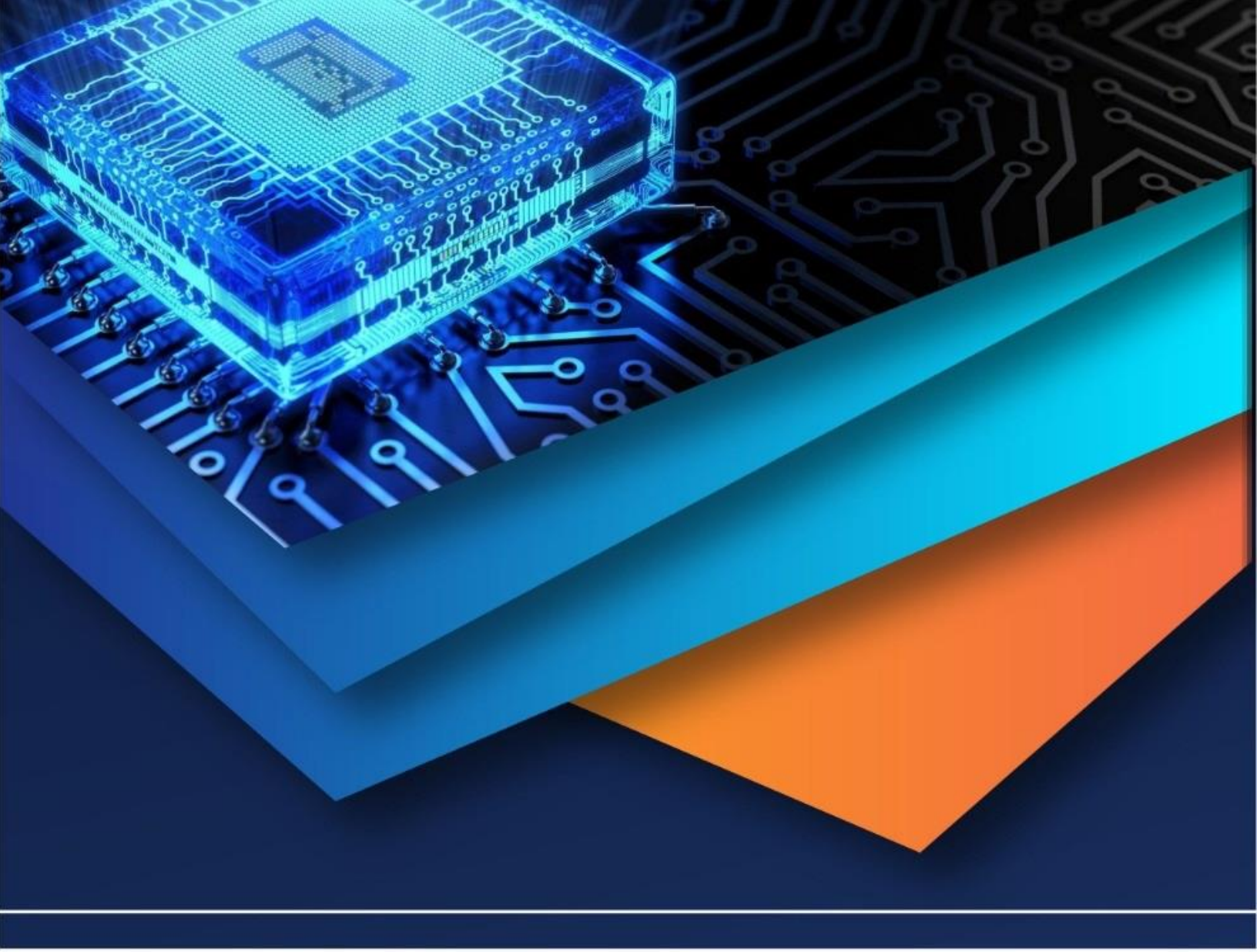
[16] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury "A Simulation Analysis of Flooding Attack in MANET using NS-3", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Syst,, Feb. 28 2011-March 3 2011.

[17] Humaira Ehsan and Farrukh Aslam Khan, "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs", 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[18] Ms. Arpita Raverkar, "Route Discovery in Insecure Mobile Ad hoc Network", IEEE, 2011 978-1-4244-8679-3/11/.

[19] S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam,"A Review on Attack Prevention Methods in MANET" Journal of Modern Mathematics and Statistics Year: 2011 | Volume: 5 | Issue: 1 | Page No.: 37-42.

[20] Abdur Rashid Sangi, Jianwei Liu and Likun Zou, "A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs", IEEE, 2009978-1-4244-4507-3/09/.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY