CARF-F: Conditional Active RREQ Flooding-Filter based Prevention Scheme for AODV in MANET

Neha Kamdar
M-tech Scholar
Department of Computer Science & Engineering
Oriental University, Indore (M.P), India

Neeraj Paliwal
Associate Professor
Department of Computer Science & Engineering
Oriental University, Indore (M.P), India

ABSTRACT
Wireless network is a growing field of latest technology because of its increased popularities over the rural and urban areas. Such network provides the mobility based service usage and hence removes the location dependencies for the users of mobile devices such as laptops, cell phones, Tablets and PDA's. These networks are categorized on the basis of their infrastructural usage and range of transmissions. Mobile ad-hoc network is one of its types having infrastructure less environment performing short range communications. In this the overall responsibility of communication is shifted from networked components to mobile node itself working as a router. As the facility is increased some relaxation is also made available for malicious users and hence it is more susceptible to network attack due to its open environment and dynamically changing nature. Flooding is used for the most performed network attack aims at degrading the network performance by inserting the several dummy RREQ packets in the network. These packets are large in quantity and hence consume lots of network resources such as, bandwidth and nodes battery power. Over the last few years various approaches is been suggested to overcome flooding related issues. Even after these traditional flooding attacks solutions, there are some problems which remain unsolved like: isolation of fake RREQ from actual packets, maliciousness percentage based on nodes behaviour and previous participation, probability of malicious flooded packet detections. Thus this paper proposes a novel CARF-F based flooding attack detection and removal mechanism for AODV protocol. At the initial level of analytical results the approach is proving its strong presence in near future.

Keywords
Wireless network, MANET (Mobile Ad-Hoc Network), AODV, Network Attacks, Flooding Attack, Rate Threshold Limit, CARF-F (Conditional Active RREQ Flooding-Filter).

1. INTRODUCTION
Mobile ad hoc network is a wireless network which works without any infrastructural dependencies. The nodes in MANET are connected to each other in an unstructured manner due to changing positions of mobile devices which makes it dynamic in topological nature. Each node will travels in any of the expected directions of motion frequently and routing is controlled by the node itself due to its inbuilt router capabilities. It is an autonomous network might be connected to Internet through some other nodes. The primary operational functionality of the mobile nodes is to make the communication with some other node when desired and sustains the connection characteristics for required durations. Some of the application areas of MANET are: collaborative work, crisis management, personal area network etc. Concern is to provide the effective shorts range communication without any device requirement other than mobiles. MANETs have a number of characteristics and challenges which are dynamic topologies, Bandwidth-constrained, variable capacity links, Energy-constrained operation, Security and so on [1].

Over the last few years lot of research had been take place to support the above characteristics using various routing protocols and conditions. The routing work is categorized by its protocols which fall in the category of reactive or proactive. Some of the protocols are AODV, DSR, TORA, DSDV etc [2]. These protocols provides the basic functionality related to route discovery, connection establishment, link handling, shortest path, secure transmissions, optimal flow, load balancing, overhead reduction, and maximizing throughput.

Among them security is the most essential feature needs to be provided for effective communications and will cost considerable damages if neglected. Estimating and implementing security constraints with existing protocols had gain interest of many researchers. Various new techniques are suggested to overcome the loopholes in mobile security and made improvements catastrophically.

Security defines the mechanism to handle undesired operations in specifically generated conditions to degrade the network performance. These planned conditions are known as attacks. Due to the dynamic nature of MANET, it is affected most by the attackers. There are so many attacks like, black-hole, wormhole, flooding, packet drops, masquerade etc which creates misbehaving nodes in the network whose aim is to let the network actual functioning down. Security is mainly involved with military applications using ad-hoc networks in critical conditions. Thus a network is taken as a secure if it holds following properties for transmissions [3]:

i. Availability: Ensures that the network manages to provide all services despite when denial of service attacks occurred intentionally.
ii. Confidentiality: Ensures that certain information is never disclosed to unauthorized users in any routing scenario.
iii. Integrity: Guarantees that the message that is transmitted reaches its destination without being changed or corrupted in any way.
iv. Authentication: Enables a node to be sure of the identity of the peer with which it communicates.
v. Non-repudiation: Ensures that the originator of a message cannot refuse sending this message.

This paper gives a brief study over the flooding attacks and focused to develop some defending mechanism against them. The paper is divided into three major sections. Section-I includes basic details covering with introduction and background. Section-II describes the previous work and

problem still remain unsolved in those. Section-III proposes a solution to overcome flooding and the evaluation of the suggested approach.

2. BACKROUND

Network is categorizes by its nature to serve communication: wired or wireless. As the number of mobile devices is increasing, the communication characteristics due to motion is also gets complicated with increase in users quantity. Supporting such behaviour can be made possible by various short range infrastructures less networks. Mobile ad-hoc network is one of the networks having zero dependencies of infrastructure and works for short range communications. It is always vulnerable to attacks because of its variation in working environments and open communication mediums. Mobile ad hoc network is one of those networks susceptible to attacker's activity and causes sudden drops. As the environment is mobile device based so the nodes are regularly coming and leaving the network which gives a space to maliciously behaving node to take the participation in communication. Thus in presence of these malicious nodes the primary focuses is towards the development of robust security mechanism to deal with attackers. During the last few years several authors had worked to improve such situations and suggested mechanism to overcome these issues. This work focuses towards security of AODV protocol from denial of service based flooding and ad-hoc flooding attacks.

2.1 Understanding Flooding Attack

It is the network layer attack planned to increase the network and node resources consumptions such as bandwidth and battery life to affects the normal processing and request. It is the most devastating category which makes the network congested due to numerously generated dummy request RREQ packets. These are RREQ's are flooded in a network to make the connection request heavily that it was no longer processing the request of even actually desired nodes [4]. The aim is to create overhead for the network and thus the actual legitimate request gets affected. From this numerous request the connection buffers gets filled completely and after a time limit the results in denial of service (DoS) zone. Flooding can be categorized by its targeted systems and attack generation systems such as normal flooding (DoS attack), specific targeted flooding, distributed denial of service (DDoS) flooding, ad-hoc flooding etc.

2.2 Attack Scenario

These flooding mechanisms will consume the network through multiple RREQ packets and will be detected by secure AODV through a rate limitation (RREQ_RATELIMIT) mechanism. This rate limit will work as limitation on sending the request packets to the network per unit time. If a node broadcasted a RREQ then it needs to waits for RREP until the response came. If the response is not reached then a node will again send RREQ packets up to its overall time to live values (TTL). These repeated attempts of sending RREQ to the network again and again will consume the resources and causes degradation in the performance of network termed as exponential drops. Also if the mass RREQ packet is coming in smaller time, the storage table at the node will be filled earlier than its time causes drops in later request which might be from legitimate node.

2.3 Effects of Flooding Attacks

As flooding attacks is related with resource consumption of node and network both then the evaluation of its affects is also at the dual end. It degrades the performance of reactive strategies and protocols in the following way:

2.3.1 Buffer Performance Degradation

As the buffer is used to store the route request for a node by routing protocols, hence the flooding request make it completely filled which will later on drops the coming request packets and will jam the network due to not generation of RREP [5].It will not make the complete route discovery as the large number of packets generating from application layer is unreachable. The size and limit of buffer is decided by some management techniques but still ineffective for DDoS based flooding.

2.3.2 Interface Performance Drops

Here the interface is gain used to connect network with the system of node. And if the buffer gets overflowed this interface also might not work due to burdensome of malicious or fake packets. Legitimate packets are dropped without any priority of packets at interface.

2.3.3 Collision at MAC Layer

Numerous RREQ packets not only make the network down, but it also lets the normal traffic jams and collided because of these heavy loads. Flooding packets consumes more bandwidth than actual packets results in congestion and collisions of packets. It also affects higher layer sensitive protocols such as TCP with this congested environment. The paper [6] shows some of the basic flooding prevention schemes for above attacks.

2.3.4 Overall MANET Performance Degradation:

Due to such uncertain and heavily loaded environment, the consumption of network and node resources is increased exponentially causes the performance down. Flooding attacks affects power consumptions, bandwidth utilizations, links failures, network lifetime reduction, overhead increase etc.

3. LITERATURE SURVEY

Over the last few years multi variations of flooding attacks is measured in the ad-hoc networks. The aim of those attacks is to occupy or consume the resources so as to affects the normal working of the network. Various mechanism to overcome such attacks categories is been suggested and resolves various issues related to flooding attacks. Out of those some of the identified approaches which leads us to fulfil the research task is submitted here as literature survey. The brief overviews about the approaches are and papers are given below.

In the paper [7], denial of service (DoS) based attacks categorization and identification strategy is given. According to the paper, the DDoS attacks from malicious nodes can be initiated by forwarding the fake route request packets which leads towards the network consumptions. Such attacks are hard to detect because of their sudden behaviour change. Here in the network, attacker's node performing route discovery more frequently than the other nodes. It could be detected by a distributed filtering scheme by which throughput degradations are identified. The paper assumes a 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. The proposed technique uses a filter to detect misbehaving nodes and reduces their impact on network performance.

In the paper [8], an obligation-based model called fellowship is proposed to mitigate the flooding and packet drop attacks in ad

hoc network. The model is capable of identifying and removing both malicious and selfish nodes. The approach is able to detect packet dropping and flooding attacks by using two techniques: Rate limitation and Enforcement. In accumulation, the method does not rely on any federal authority or tamper-proof hardware devices. The obligation for the involvement is relative to the node's potential resources, the period it stays in network and the type of connection it has with the nearest neighbour's nodes and gateways.

Some of the authors had worked with historical participation using trust based mechanism for flooding attacks detections and preventions. In process of that, a novel technique to mitigate the effect of RREQ flooding attack using trust assessment function is proposed in paper [9]. The proposed approach is a distributed cooperative model in which all the node locally run the intrusion detection code and collaborate with each other for flooding preventions by using three method functions of relationship detections. These trusted relationships using stranger, acquaintance and friend, proves the participation nature of a node in a network. Similar representation of trust based detection is also given by paper [10] along with complete evaluations of results under the different conditions of attack nodes, flooding frequencies, bandwidth and topologies.

In this paper [11], a study and evaluations of flooding attacks is suggested by giving some detection parameters. Here the various parameters will work as a single mechanism for detection of DDoS attacks and distributive flooding attacks. The paper in its later section also suggests an explicit query based detection and prevention technique for DDoS. These parameters are: sequence number, battery power, RTT, threshold values, packets forwarded at each node, total time taken by any packet, black-list and a notification mechanism (EAN). At the primary level of simulation study the approach is proving its effectiveness.

In the paper [12] is suggested to deal with attack impact and later on give some improvements over the detection environments. The paper is majorly studying the attack influence by monitoring its transmissions. In the network when a node is start forwarding the RREQ packets than first its behavior is analyzed by which decisions making related to its attack confirmation is provided. Proposed technique to implement prevention mechanism is by disabling IP broadcast used in AODV routing process. Flood attack occurs because of initiating lots of packets in the network so that network becomes congested and no bandwidth is available to send packets and the approach is capable of detecting it.

In the paper [13], author proposes a novel defence mechanism using the amount of legitimate packet processing at each node by which collaborative flooding attacks detection rates are improved. The work also resolves a network conditions and confirms that flooding attacks not only causes network down but also restrict the process of legitimate nodes. The work also estimates the quality of the packets by using two specific buffer corresponding sizes of control packets buffer and the data packets buffer. The local density of a node is defined as the number of neighbouring nodes lying under its transmission range. The simulation results show that the proposed scheme also improves the end-to-end packet delivery ratio.

The paper [14], analyses the flooding and packet dropping attacks for the anonymous communications in ad-hoc networks. The paper also suggests a novel technique to identify the flooding malicious node and is capable to provide a distinction between actual packets and attacked packets. The approach isolates the malicious node packets from the normal node by using a behaviour analysis mechanism using rate limit transmission module. To achieve this, the rate-limitation at every node uses a threshold-tuple, which is a list of thresholds. Taking about the effectiveness of the approach, the number of packets for the approach is also less as compared to other existing mechanism thus the overhead associated with the approach is better than others.

4. PROBLEM STATEMENT

Flooding is the active category based network attack whose aim is to make the network congested by some fake route request (RREQ) packets. In this scenario when a route initiated route discovery then the source node sends RREQ packet to its neighbors and waits for a time for its reply. The node is not having any information about the behavior of its neighbor. The neighbors distance is taken as a hop count. Thus if the node is having smallest hop count the packet is forwarded to it. During this process of traditional routing the verification of legitimate node condition is not involved and hence some new node will destruct the actual working of the network by flooding the fake RREQ packets to the network. By this packets the actual packets route discovery gets affected and which later makes denial of service (DoS) attacks. Thus in absence of any malicious packet removal schemes the network is gets congested with these fake packets. Traditional schemes are not capable of identifying these packets. So later on several improvements over the AODV protocol is proposed. This paper studies various techniques proposed for overcoming the flooding attacks situation and measured that there are some issues which remains unsolved. These issues are taken as problem statement of this work and given as:

Problem 1: Te legitimacy condition of node is not defined before Route Discovery. Thus malicious node will be able to take participation in flooding attack generation.

Problem 2: Flooding packet detection is not taken into combination with the malicious node removal. Both are having the same goal of dropping the networks performance and separate mechanism will consumes more resources.

Problem 3: Traditional Rate limiter will only controls the flow but the categorization of flow is not performed which includes the isolation of normal RREQ and fake RREQ.

Problem 4: Existing mechanism provides one time solution when recovery is started. Thus some regular monitoring schemes are required for further improvements.

This out of the various positive outcomes of existing mechanism, there are some unaddressed issues which needs to be resolved for complete solution. Thus this work proposes a novel CARF-F based flooding attack removal in MANET which will serve the needs of security.

5. PROPOSED CARF-F APPROACH

This paper proposed a novel Conditional Active RREQ Flooding Filter (CARF-F) based flooding attack detection and removal technique. The approach provides effective detection by minimal overhead messages in the network. Flooding is an uneven and undesired consumption of networked resources by sending fake RREQ packets in the network and comes under the active category attack. The aim here is to unnecessarily consume the network bandwidth and nodes battery by which actual transmission gets affected and overall network gets degraded in its performance. Over the surveyed paper various mechanism is been proposed to overcome such conditions but increases overhead by detection packets. Also the conditions are quite computational burden oriented and complete detection of flooding node with flooded packet removal is not given as a single element. The CARF-F based approach restricts the nodes for limited transmission in certain attack generation conditions

by which the attacker nodes vulnerability gets reduced. Thus it is more likely working as packet filter mechanism by selective forwarding process used for fake packets. In the below figure 1 initially the nodes start routed discovery by sending the RREQ packets to its entire neighbour. The sender waits for its reply. During this period the attacker's node will also transmit fake RREQ whose aim is to make the network congested. Now this fake RREQ will forward to the entire neighbour. In absence of any detection mechanism these packets are multiplicatively forwarded which after some time gets the network overall bandwidth consumed and will affect the working of actual route discovery process of normal node. CARF-F provides two basic conditions as an improvement over above flooding mechanism.

First, it blocks the flooded RREQ packets to be further transmitted by a packet rate limiter with a conditional threshold values.

Second, it detects the fake RREQ generation node which later on removed for further futuristic security over such attacks.

The architectural functionality represents the goal achievement of the proposed CARF-F on different attack conditions. The work is takes as parameter detection because it identifies various attack detection parameters and on the basis of which the packet is confirmed to be attacker or not. The detailed working of above figure is clarified by its components descriptions. Thus the proposed CARF-F approach is suggested using three major components functionalities. These are:

5.1 Conditional active RREQ Flooding Filter

This component will work as limiter for the network. It provides the multiple conditional checks by which the packets flows have to go through. The filter is capable of holding packets for a fixed time before forwarding it to other nodes. During this time several networked components and behaviour detection can be performed. Like the congestion is the network so packet can be stored on to some temporary buffer until the network congestion gets reduced. The filters have a fixed buffer size for intermediate nodes packet storage.

5.2 Flooded Packet Removal

During the filtration operation the CARF-F filter also perform this functionality of fake RREQ removal from the network. According to the filter operation each node can overhears its neighbour transmissions. In this overhearing the total number of packets relayed is stored as a behavioural element of the node. Now the component categorizes received and other packets from route discovery RREQ packets and checks their count. If the count of RREQ packets on this node is greater than a defined threshold limit, the packet is dropped considered to be a fake RREQ packet from malicious node. After removing the fake packet the counter flag bit value is set to zero. For each successful removal the counter flag value is decreased by one. And for each successful packet forwarding to other nodes it is set to one and later on increased.

Here the primary task is to design the rate limit threshold value. It can be measured by previous participation of node in successful transmissions. If the value of relayed is more than threshold value than the packet if forwarded further as a actual packets. Hence by this component the fake packets making the network congested is removed effectively. This component has a conditional verification of routing process and uses a most effective filed such as the TTL value. His component will also make the process fast due to its less overhead involvement and message communications.

5.3 Flooding Node Removal

This module's major functionality is to remove the flooding RREQ generating node. After the flooded packet removal the destination adders of requesting RREQ node is taken for verification of flooding generation node. Now authenticity of this node is checked by a Hello packet. The node sends a Hello packet to the address and waits fro a reply. If the reply is not received than it is confirmed to a flooding attack node. The reply is also checked for a time period having fixed TTL according the hop count value. If the condition is met then the node is marked as a flooding attacker ode and its entry is removed from outing table with an alert message to all the nodes in the network.

In this way both the aim of the CARF-F is achieved after which the flooding attack fake RREQ packet is removed and the flooding attack generator node is also deleted. The approach is capable of overcoming the multiple situations of denial of service attacks and distributed denial of service attacks. Later on observation of the components feature analytically, it is found that it is serving the users security needs with lesser overhead associated with it.

5.4 Expected Benefits

i. The scheme is capable of timely malicious behavior detection and continuous monitoring which saves network resources efficiently.
ii. The flooded nodes and packets are detected and removed using conditional threshold based rate limiter.
iii. Alerting mechanism makes the difference between the actual node and attackers node by which categorization is made easy.
iv. Collaborative flooding is also detected by the approach and gets isolated by other nodes preventing DoS, and DDoS attacks
v. No extra overhead is involved with the CARF-F and it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV.
vi. Also, the proposed scheme is more efficient in terms of its resultant routes established, resource reservations and its computational complexity.

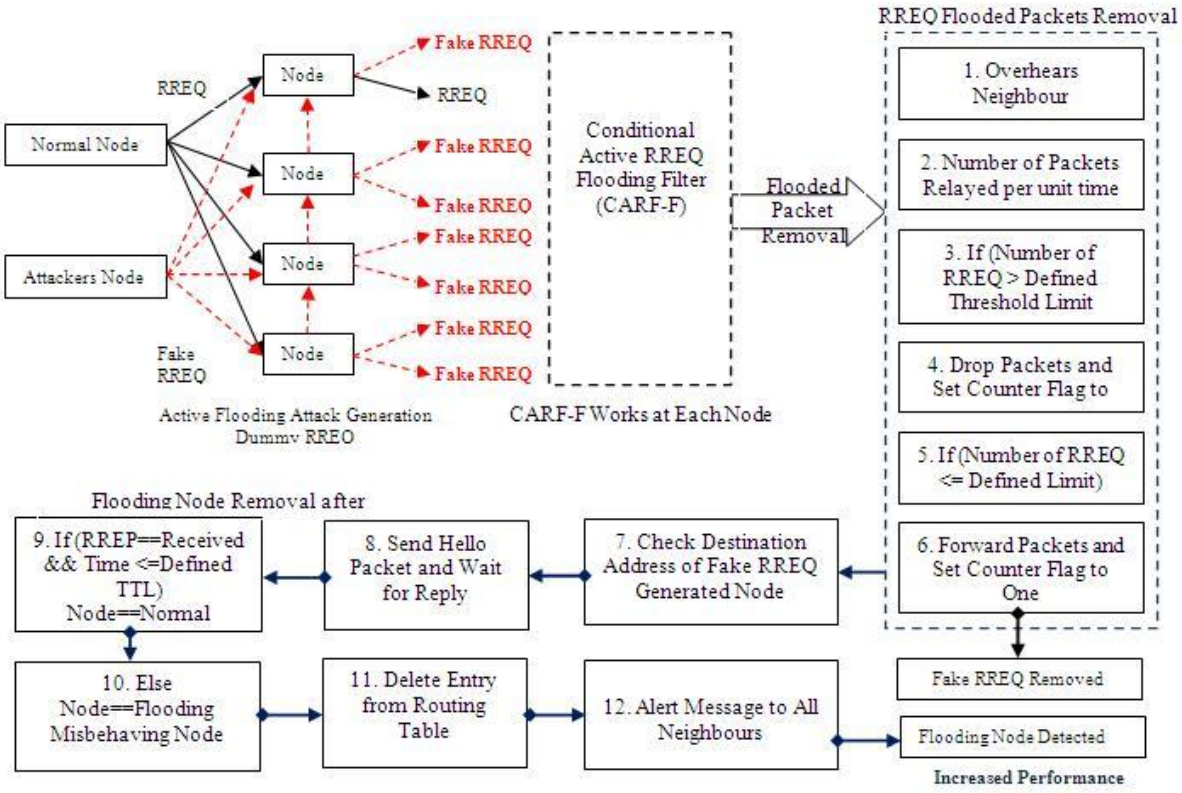

Figure 1: Proposed CARF-F Based Flooding Attack Prevention and Removal Technique

6. PERFORMANCE METRICS

As the proposed CARF-F based flooding attack detection and removal approach is proceeds promisingly but to prove its effectiveness and results some of the existing evaluation parameters are required. For this work following are some quantitative metrics used to evaluate its performance against DoS and DDoS attacks. These are:

6.1 Packet Delivery Ratio (PDR)

It is the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received. This number represents the effectiveness and throughput of a protocol in delivering data to the intended receivers within the network.

6.2 Packet Loss Rate

The ratio of the number of packets dropped by the nodes divided by the number of packets originated by the application layer continuous bit rate (CBR) sources. The packet loss ratio is important as it describes the loss rate that can be seen by the transport protocols which in turn affects the maximum throughput that the network can support. The metric characterizes both the completeness and correctness of the routing protocol.

6.3 Number of collisions

In a network, when two or more nodes attempt to transmit a packet across the network at the same time, a packet collision occurs. When a packet collision occurs, the packets are either discarded or sent back to their originating stations and then retransmitted in a timed sequence to avoid further collision. Packet collisions can result in the loss of packet integrity or can impede the performance of a network. This metric is used to measure such collisions in the network.

6.4 Throughput

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps) and sometimes in data packets per second or data packets per time slot.

6.5 Average delay

Average of delays incurred by all the packets which are successfully transmitted.

6.6 Average number of hops

Total length of all routes divided by the total number of routes. Although behave legally, cannot set up paths to send data.

Thus in near future after the implementation in NS2, the approach will definitely proves its results on above parameter. At the initial level of analytical reasoning and evaluations the approach is proving its efficiency than other approaches.

7. CONCLUSION

Mobile as hoc network is widest range of protocol working towards security but there needs some improvements over the dynamic and active category of attacks. Out of these the flooding attacks will proved to be devastating in terms of

resource consumption in terms of bandwidth and battery power of the nodes. As the MANET is not having any infrastructure and if all of a sudden due to such flooding affect the networks performance gets degraded and the actual operations of communication will be terminated. This paper addresses some of the issues which remain unsolved in respect to flooding attacks. The paper also proposes a novel CAR-F based flooding attack detection and removal. The approach is capable of removing the flooded packets and even the node from which flooding gets started. The less overhead and consumption based detection makes the approach a competitive solution. At the primary level of analytical study and calculation of CARF-F evaluation, it looks that the proposed scheme will shows its strong presence in near future.

8. ACKNOWLEDGMENTS

The authors wish to acknowledge college administration for their support & motivation during this research. The authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. They also like to give thanks to Proff. Neeraj Paliwal for discussions in specific domain.

9. REFERENCES

[1] D. Karun K Reddy, K. Sandhya R Kundra, M .Ratnakar Babu, Dr. L.Prassana Kumar, "Prevention of Routing Attack in Mobile Ad-Hoc Networks: A comparative study, in International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol. 1, Issue 5, October 2012.

[2] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", in Journal of Computing, ISSN 2151-9617, Vol. 3, Issue 1, Jan 2011.

[3] Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G. and Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks", by Embedded Systems Research Group, Tata Consultancy Service s, Bangalore-560066, India.

[4] Isa Maleki1, Ramin Habibpour, Majid Ahadi and Amin Kamalinia, "Security in Routing Protocols of Ad-Hoc networks: A Review", in International Journal of Mobile Network Communications & Telematics (IJMNCT), doi: 10.5121/ijmnct.2013.3403, Vol. 3, No.4, August 2013.

[5] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", in Wireless Mobile Network Security, Chapter 12, Springer, 2006.

[6] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", in International Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN: 2249-6343, Vol. 1, Issue 3, 2012.

[7] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", in IEEE Computer Society , ISSN:0-7695-2736-1/06, 2006.

[8] Venkatesan Balakrishnan, Vijay Varadharajan and Udaya Kiran Tupakula, "Fellowship: Defense against Flooding and Packet Drop Attacks in MANET", in INSS Research Group, Department of Computing, Macquarie University, North Ryde, Sydney, NSW Australia 2109

[9] Shishir K. Shandilya and Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", in International Journal of Computer Application, ISSN: 0975 – 888, Vol. 5– No.12, August 2010.

[10] Ujwala D. Khartad & R. K. Krishna, "Route Request Flooding Attack Using Trust based Security Scheme in Manet", in International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248- 9738 Volume 1, Issue 4, 2012.

[11] Neha Singh, Sumit Chaudhary , Kapil Kumar Verma and A. K. Vatsa , "Explicit Query based Detection and Prevention Techniques for DDOS in MANET", in International Journal of Computer Applications, ISSN:0975 – 8887, Vol. 53– No.2, September 2012.

[12] Meghna Chhabra and B.B. Gupta, "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)", in Research Journal of Applied Sciences, Engineering and Technology, ISSN: 2033-2039, Vol. 7, Issue. 10 March 2014.

[13] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks", in Journal of Information Processing Systems, DOI : 10.3745/JIPS.2011.7.1.137, Vol.7, No.1, March 2011.

[14] Venkat Balakrishnan, Vijay Varadharajan, and Uday Tupakula and Marie Elisabeth Gaup Moe, "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", in Information and Networked Systems Security Research (INSS) Group, Department of Computing, Macquarie University, Sydney, Australia

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