AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Transmission Sequence Based Packet Scanner Detection For Flooding Attack Using DSR Based MANET

[1]M.D.Vimalapriya and [2]Dr.S.Santhosh Baboo

[1]*Research Scholar, Sathyabama University,Chennai, India*
[2]*Associate Professor, Post Graduate and Research, Department of Computer Applications, D.G.Vaishnav College, Chennai, India.*

ARTICLE INFO

Article history:
Received 2 March 2014
Received in revised form
13 May 2014
Accepted 28 May 2014
Available online 23 June 2014

Keywords:
Data flooding attack, denial of service, DSRprotocol, Transmission sequence based packet scanner, MANET.

ABSTRACT

Background: Mobile Ad hoc Network (MANETs) are relied upon to be broadly utilized as a part of the not so distant future. In any case, they are powerless to different security threats due to their characteristic qualities. Many denial of service attacks are possible in MANET and one of these type of attack is flooding attack in which attacker exhausts the network resources such as bandwidth and to consume a node's resources such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. Flooding attack is possible in almost all on demand routing protocol.**Objective**:In this paper present a technique to mitigate the effect of data flooding attack in MANET using Transmission sequence based packet scanner(TSBPS) technique in DSR on demand routing protocol.**Result:**The new scheme utilized a four way detection method of National based Intrusion Detection System (NIDS) to detect a flooding attack and suppressing the influence of the attack effectively. **Conclusion:**The simulation results show that the proposed scheme detrimental effects of flooding attack and also improve the packet delivery ratio and decrease a end to end delay.

To Cite This Article: M.D.Vimalapriya and Dr.S.Santhosh Baboo, Transmission Sequence Based Packet Scanner Detection For Flooding Attack Using DSR Based MANET. ***Aust. J. Basic & Appl. Sci.,*** *8(9): 64-71, 2014*

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are structured powerfully by an independent arrangement of nodes that are joined by means of remote links without utilizing the current system base (Imrich Chlamtac, *et al*.,2003).The nodes in a specially appointed system can correspond with any viable node that stays inside its transmission range. For conveying past its transmission extends, the nodes use intermediate nodes to achieve destination (V.Gupta, *et al*., 2002). The primary destination of a routing protocol is proficient disclosure and stronghold of a course between the source and the destination so that there could be an opportune and effective conveyance of data between them. The reactive routing protocol DSR (C.E Perkins, E.M Royer,2001) invoke route discovery on demand. As such just when node needs to send data to its companions the course is uncovered by the protocol. It doesn't require the nodes to keep up courses that are not eagerly utilized for correspondence.

The Flooding attack (R.H. Khokhar et, al.,2008) is launched at the network layer by the malicious node. It sends massive amount of control packets to the network. This attack aims at depleting the network resources like bandwidth, battery power and thereby preventing the network from providing services to legitimate users. The flooding attack can target the victim node or the network as a whole. In case of RREQ flooding attack the malicious node imitates like normal node in all aspects, except in performing unnecessary route discoveries. These malicious nodes frequently initiate route discovery to destinations with the intent to flood the network with route request packets. As it is difficult to distinguish between a route discovery initiated with a malicious intent and a legitimate route discovery for repairing broken/stale routes, this type of attack is hard to detect.

The system asset like transmission capacity (bandwidth) is adversely influenced by Flooding attack propelled in DSR based MANET. The same is examined through reproduction brings about Examination of Impact of Flooding attack on MANET and to highlight on Performance debasement (Bhuvaneshwari K, et, al.,2013) delineating the criticalness of location of Flooding attack in MANET.

The DSR protocol is used to detect the Flooding attack in Mobile ad hoc networks. In this paper, to overcome the flooding attack using Transmission sequence based packet scanner algorithm. This paper concentrates on the performance of Dynamic Source Routing (DSR) routing protocol under flooding attack, by

Corresponding Author: M.D.Vimalapriya, Research Scholar, Sathyabama University,Chennai, India
E-mail: prshvi@yahoo.co.in

observing and analyzing the network's packet loss rate, average end-to-end delay and throughput. Now, DSR has already become one of the classical Ad Hoc routing protocols and is widely used in Ad Hoc Networks and new emerging Wireless Mesh Networks (WMN) (Akyildiz, I. F.,Wang, X.,2005) as well. Consequently, our research on the security and reliability of DSR is of practical importance which provides a solid foundation of further research.

The remainder of this paper is organized as follows. In Section 2, provides the related work in MANET and section 3, describe an overview of DSR protocol and flooding attack on DSR routing protocol. In Section 4, the proposed method is presented and simulation results are given in Section 5. Conclude the paper in Section 6.

Related work:

Essential work has done in securing the ad hoc network. Some researcher defined the process for secure routing, but it cannot able to handle the flooding attack.

The author (Vijay Varadharajan, and Uday,2007) investigated the flooding attack in unacknowledged correspondence. They utilized the threshold tuple which comprise of three segments: transmission threshold, blacklist threshold and white listing threshold. In the event that any node produces RREQ packet more than transmission threshold, then its neighbor tosses the packet on the off chance that it crosses the transmission threshold more than blacklist threshold then it boycott the node. Be that as it may to manage coincidental blacklisting, they characterized white listing threshold. In the event that any node performs well for various interims equivalent to the white listing threshold, then it again begins treating as a normal node.

In the paper (Revathi Venkataraman, et, al., 2009), utilized the broadened DSR protocol focused around the trust function to alleviate the impacts of flooding attack (Theodorakopoulos and Baras, 2006). They sorted the nodes in three classifications: Friends, acquaintance and stranger. The stranger is the non-trusted node, companions are the trusted node and acquaintance has the trust values more than stranger and short of what companions. In view of the relationship they characterize the three threshold values. In the event that any node accepts the RREQ packets, then checks the relationship and focused around that it checks for the threshold esteem in the event that it is short of what the threshold, then send the parcel, overall toss the bundle and blacklist the neighbor node. The primary issue with this system is not working great with higher node portability.

In (Y. Hu, et, al.,2002), which is intended for DSR networks, route discovery chains are utilized to rate-limit the amount of route disclosures. Each one route discovery needs a key from the route discovery chain and the arrival of keys might be controlled. This limits the effect of RRFA on the system, yet a settled number of produced Rreqs can even now be infused into the whole system. Moreover, honest to goodness RREQ endeavors from a traded off hub to the reachable ends might never be sent if the amount of fashioned Rreqs generated by it is vast.

The author (P. Yi, et, al.,2005) dissected the Flooding Attack Prevention (FAP) plan has tended to the noxious flooding attack and proposed a guard framework, being the first to do so. They propose the neighbor concealment mechanism for the RREQ flooding attack and the way cut off mechanism for the information flooding attack. In the neighbor concealment mechanism, they focus the necessity of neighboring hubs by opposite extent to its recurrence of starting RREQ bundles. The threshold is controlled by the most extreme number of starting RREQ parcels in a certain time period. In the event that a neighboring hub advances more RREQ parcels than the threshold, the getting hub basically denies them. Notwithstanding, the neighbor concealment mechanism does not check whether it accepts the relating RREP parcel or not. Subsequently, counteractive action from inaccessible end (R. Kumar, et, al.,2006)is not conceivable. It is likewise defenseless against the RREQ flooding attack directed by the era of numerous diverse source addresses. To keep from the information flooding attack, the way cut off mechanism cuts the way off when the amount of accepted information parcels from one neighboring hub surpasses the threshold. Thus, the way over which real bundles are exchanged is likewise detached because of the suspected neighboring hub.

(S. Li, Q. Liu, et, al.,2006)proposed the Avoiding Mistakes Transmission Table (AMTT) plan (Akyildiz, I. F.,Wang, X.,2005)recommends a barrier framework against the malevolent flooding attack by using an evading mixed up transmission table. The AMTT plan requires gigantic memory space and extensive transforming time for sparing the packets at every node.

(Jian-Hua Song1, et, al., 2006)the author proposed the distributive approach to resist the flooding attack. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less then BLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less than BLACKLIST_LIMIT then put the RREQ in the delay queue andprocess after queue time out occurs. This method can Handel the network with high mobility.

Background:

Overview on Dynamic Source Routing Protocol:

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. DSR maintains a route cache, which leads to memory overhead. Then DSR maintains a routing table, which stores the each node information and the next hop information/address. There are two important mechanisms in DSR: Route discovery mechanismand Route maintenance mechanism, which discover and maintains a source route to random destinations in the ad hoc networkroute to the destination. DSR protocol is popular reactive routing protocols.

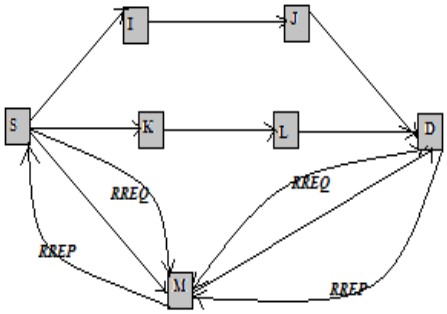

Fig. 1: Route Recovery Process

The Route discovery mechanism is used to find the route between the sender and the receiver. In this mechanism, consider the Fig.1., a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to destination node D and it does not already know a route to D(Imrich Chlamtac, *et al*.,2003). S will obtain a suitable source route by searching its Route Cache of routes previously learned, but if no route is found in its cache, it will initiate the Route Discovery protocol to dynamically find a new route to D.

To initiate the Route Discovery (David B. Jhonson , et, al.,) the source transmits a ROUTE REQUEST (RREQ) message to all nodes within wireless transmission range of source. Each RREQ also contains a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded. When another node receives a RREQ, if it is the target of the Route Discovery, it returns a ROUTE REPLY (RREP) message to the initiator of the Route Discovery. When the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. If it finds that its own address is already listed in the route record in the RREQ message, it discards the REQUEST.

Route Maintenance(David B. Jhonson , et al.,)is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D. Route Discovery and Route Maintenance each operate entirely on demand. When all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. In response to a single Route Discovery, a node may learn and cache multiple routes to any destination. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks. The DSR protocol is a secure, efficient approach for the detection of the Black hole attack and Wormhole attack in the Mobile Ad-hoc Networks.

Description of Routing Attack on DSR Protocol:

Flooding attack:

Flooding is a Denial of Service (Dos) that is designed to bring a network service down by flooding it with large amounts of traffic. Flooding attack occur when a network or service becomes so weighed down with packets Initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or a host with connections that cannot be completed, the flood attack eventually fills the host memory buffer. Once this buffer is full no further connections can be made, and the result is Denial of Service. The flooding attack is possible in almost all on demand routing protocol (DSR) (Imrich Chlamtac, *et al*.,2003).

Proposed Techniques:

Transmission Sequence Based Packet Scanner:

Flooding attack is one of major problem in a mobile ad-hoc network while communication between source and destination. This is occurred when an attacker sends an excessive data to a network resource and override the bandwidth capacity of the communication link by adding extra pockets (empty pocket) at the time of transmission. To overcome this problem, the proposed approach utilized a four way of detection of a flooding attack based on NIDS (National based Intrusion Detection System)as follows:

i) Empty packet detection
ii) Detection based on source id
iii) Detection based on number of hops
iv) Detection based on transmission sequence number

Empty packet Detection:

The number of packets transferred between source and destination at any network link with a fixed bandwidth capacity. Observe each packetcontent size with their bandwidth capacity of a link transferred from source to destination. An attacker can be traced at any link before it reaches the destination by adding an empty packet. Through a proposed algorithm, destination node can easily identify the empty packets and discard it.

Detection based on Source ID:

The source node sending packets to destination node with its header information such as source id, destination id and transmission sequence number.In some cases, the destination node receives hidden source id packets from the source node. Attacker can be traced at any packets before it reaches the destination by inserting a fake source id. Using a proposed algorithm, destination node consider that the packets (hiding the source id) as a substitution packets and maintains that packets in the substitution list with the help of header information. It compares the number of packets transferred between source node packets (α) and destination node packets (β). Destination node receives an extra packets as compared to the needed packets When α is greater than β. Based on the comparison the substitution packets are discarded from the destination node as shown in Figure 2. In such a way the destination node can easily detect the malicious node.

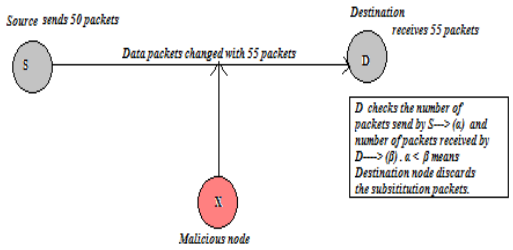

Fig. 2: Detection Based on Source id address

Detection based on number of Hops Involved:

Source node transferred the packet to destination through a number of hops present in the link. Here destination node compares the hops information with the source node. If hop information is not equal to source node then it is identify there is an attacker utilizing a hop between source and destination. *Then the destination node checks the hops using source id and detects an attacker hop effectively.*

Detection based on Transmission Sequence number:

The number of packets transferred one after another with a predefined delay includes a unique id to identify the packet at any link. This unique link is called sequence number. Observe the packet with their sequence numbers in each link. A packet can be traced at any link before it reaches destination using the sequence number. Consider an attacker between source and destination (usually flooding starts after data transfer is initiated from source). For example as shown in fig. 3, if the destination receives the packets with sequence numbered as 1, 2, 3, the attacker's packets may not possess the same order. Device and functionality that checks this ordering of packets on each entry at the destination. The function must broadcast information about unordered packets to the source. The unordered packets can be either of the following:

a. Attacker and source send a packet with same sequence number.
b. A null packet with ordered/ unordered sequence number.
c. Attacker sends a random packet order but sometimes matches with the source.

Finally the sequence number at the destination must be nullified after passing a ACK with the same sequence number (can be windowing also) to the source.

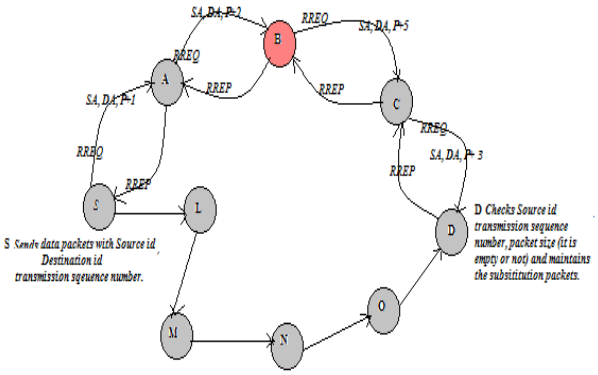

Fig.3. Flooding Attack

Pseudocode For Transmission Sequence Besed Packet Scanner:

Init P from S to D
If {id==D} {
Call observe ()
}
Else
Route to destination
Observe()
{
For all packets from S→ D
Read SN
Store O[i]← SN(i)
If AK(i) then
SN(i)=0
AK[i]=AK[i]++
//Windowing
If {AK(i)to AK(n)}
{
Store O[i]←S(n)
Check if P(i+n)=S(n+1) then
SN (i)to SN(n)=0
AK[i] =AK[i]+AK[n]
}
Case1: Attacker and source send a packet with same sequence number
Observe()
{
For all packets from S→ D
Read SN(S)
Read SN(A)
If SN(S(i+1)) is next of SN(S(i)) then
Store O[i]← SN(i)
Else
Store O[i]←Null
}
Case2: A null packet with ordered/ unordered sequence number.
Observe()
{
For all packets from S→ D
Read SN(S)
Read SN(A)
Check if P(S)!=null or P(A)!=null
//Proceed the store of the packet which is not null
}

Case 3: Attacker sends a random packet order but sometimes matches with the source.

Observe()
{
For all packets from S→ D
Read SN(S)
Read SN(A)
Check if O[i]==SN(S(i)) or SN(A(i))
If O[i]==SN(S(i)), discard SN(A(i))
}
Where, O→sequence order
SN→Sequence number
A→Attacker
P→Packet data
AK→ Acknowledgement
P(S)→ Source packet
P(A)→ Attacker packet

Advantages of the Proposed Scheme:

- Using DSR protocol in MANET will reduces overhead of route maintenance and route discovery.
- Proposed algorithm is more efficient in terms of its resultant routes established, resource reservations, packet delivery and its computational complexity.
- The proposed algorithms for improving the robustness of the Mobile Ad Hoc Networks using DSR protocol against Packet Dropping Attack, Sequence Number attack and resource consumption attack.
- In TSPS, based on the four way detection of NIDS can efficiently identify and detect a flooding attack.

Performance Evaluation:

A Simulation model was carried out using the NS-2 simulator. Mobility scenarios are generated by using a Random waypoint model by 50 nodes moving in a terrain area of 1340 x 670. Each node independently repeats this behavior and mobility is changed by making each node stationary for a short period. The simulation parameters are summarized in Table 1.

Table 1: Simulation Parameters

Simulation and Network Parameters	
Network Area	1340 x 640
Protocol	DSR
No. of Mobile Nodes	50
Network Topology	Flat Grid
IEEE Standard	802.11
Broadcasting Range	550mts
Application Type	CBR/ FTP
Application rate	1.0mb
No. of Packets	1500
Simulation Time	10s

The simulation results could be used to analyze the performance metrics of the network. The metrics are:

1) Packet Delivery Ratio: It depends upon the number of data packets that have been received successfully at the destination among the N number of data packets generated at the source.

2) Average End-to-End delay: It is the time taken for a packet to reach the destination after it has been relieved from the source. It includes all end hop time, wait time, queuing time, regeneration time and segmentation time between source and destination.

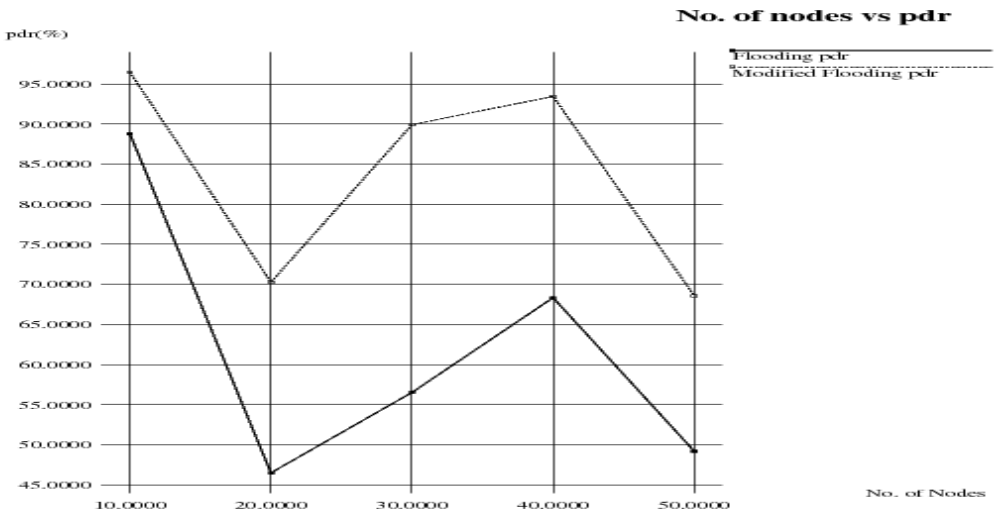

Fig. 4.a: Number of nodes Vs PDR in flooding attack

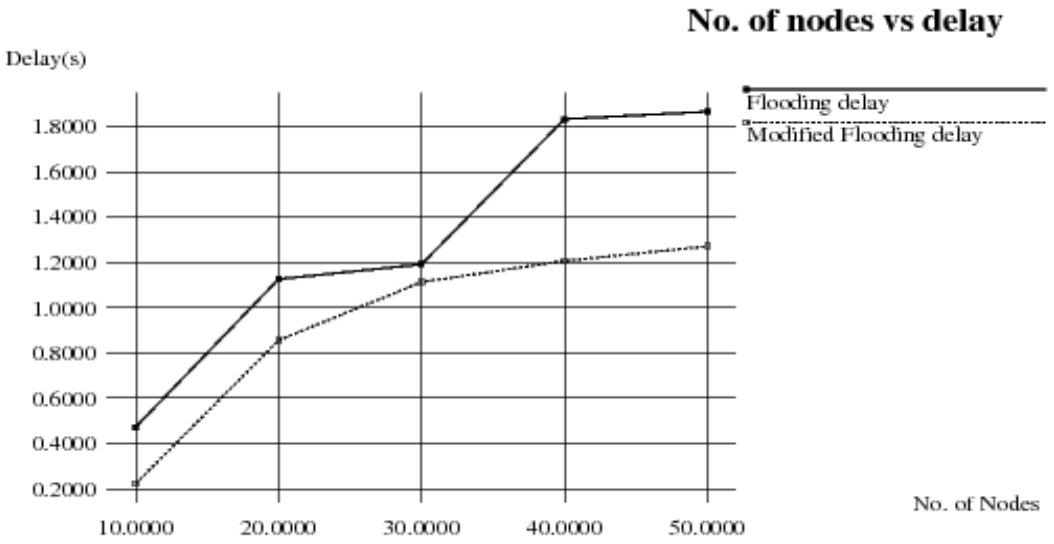

Fig. 4.b: Number of nodes Vs. End to end Delay in flooding attack

In Fig.4.a shows the performance results of Number of nodes Vs Packet delivery ratio in flooding attack. In this scenario with 50 mobile nodes, operated at a constant CBR/FTP, for a number of nodescan transfer 1500 packets, in attacked DSR protocol the delivery ratio is difficult compared to other packet delivery ratio and found to be 70% and in secured DSR protocol the delivery ratio is found to be 95%. In fig.4.b shows the performance of Number of nodes Vs delay. End-to-end delay increases if the number of packets in the network is increased. But the delay time reduced compared to the flooding delay. In attacked DSR protocol the delay is found to be 56% and in secured DSR protocol the delay is found to be 79%.

Table 2: Packet delivery ratio in Percentage

Number of nodes	FLOODING ATTACKED DSR (pdr %)	MODIFIED DSRWITH SOLUTION (pdr%)
10	88.7958	96.4824
20	46.5067	70.2755
30	56.5416	89.928
40	68.3471	93.4579
50	49.2108	68.5792

Table 3: End to end delay in sec

Number of nodes	FLOODING ATTACKED DSR (end to end delay in seconds)	MODIFIED DSR WITH SOLUTION (end to end delay in seconds)
10	0.473	0.223
20	1.126	0.856
30	1.191	1.113
40	1.832	1.206
50	1.865	1.271

Conclusion:

We have considered Dynamic Source Routing protocol for mobile ad hoc network and analyzed how the attacker can perform flooding and packet dropping in the network. Thus we have proposed a transmission sequence based packet scanner algorithm along with DSR to deal with the flooding attacks. The main advantages of our technique are that it can efficiently identify and eliminate the nodes that are flooding the network. The effectiveness of the proposed technique depends on the selection of transmission sequence number and maintaining the header information. That proposed technique is better than existing techniques. Because the transmission sequence based packet scanner algorithm used to store the source id when the source id is different from other source id. Future work of this research can be optimize the timing of sequence number searching and improve their performance.

REFERENCES

Akyildiz, I.F., X. Wang, 2005. A Survey on Wireless Mesh Networks[J]. IEEE Communications Magazine, 43(9): 23-30.

Bhuvaneshwari, K., A. Francis Saviour Devaraj, 2013. "Examination of impact of flooding attack on MANET and to accentuate on Performance degradation", International Journal of AdvancedNetworking and Applications, ISSN 0975-0290 04(04): 1652-1656.

David, B., Jhonson, David A.Maltz and Josh Broch, DSR: The Dynamic Secure Routing protocol for Multi-Hop Wireless Adhoc Networks.http://www.monarch.cs.cmu.edu.

Gupta, V., S. Krishnamurthy and M. Faloutsos, 2002. "Denial of Service attacks at the MAC Layer in Wireless Ad Hoc Networks", In Proc.of MILCOM.

Hu, Y., A. Perrig and D.B. Johnson, 2002. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proceedings of the 8th Annual International Conference on MobileComputing and Networking (MobiCom 2002), pp: 12-23.

Imrich Chlamtac, Marco conti, Jennifer J, N.Liu, 2003. "Mobile ad hoc networking imperatives andchallenges". Ad hoc networks I pages 13-64, Elseiver publications.

Jian-Hua Song1, et al., 2006. "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks " Proceedings of the Seventh InternationalConference on Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)0-7695-2736-1/06 $20.00 © .

Khokhar, R.H., Md. A.Ngadi, S. Manda, 2008. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, 2(3): 18-29.

Kumar, R., M. Misra, and A.K. Sarje, 2006. A Routing Protocol for Delay-Sensitive Applications in Mobile Ad Hoc Networks, International Symposium on Ad Hoc and Ubiquitous Computing (ISAUHC), pp: 13-18.

Li, S., Q. Liu, H. Chen and M. Tan, 2006. "A New Method to Resist Flooding Attacks in Ad Hoc Networks, International Conference on Wireless Communications", Networking and Mobile Computing (WiCOM), pp: 1-4.

Perkins, C.E., E.M. Royer, 2001. "The Ad-hoc on-demand distance vector protocol (AODV)", in Ad-hoc networking,C.E.Perkins (Ed), pp: 173-219, Addison- Wesley.

Revathi Venkataraman, et al., 2009. "Prevention of flooding attack in mobile ad hoc network". International Conference on Advances in Computing, Communication and Control (ICAC3).

Vijay Varadharajan, and Uday, 2007. Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications" The 2nd International Conference on Wireless Broadband (AusWireless) 0-7695-2842-2/07 $25.00 ©.

Yi, P., Z. Dai, Y. Zhong and S. Zhang, 2005. *Resisting Flooding Attacks in Ad Hoc Networks*, International Conference on Information Technology: Coding and Computing (ITCC 2005), 2: 657- 662.