RESEARCH ARTICLE OPEN ACCESS

Review Paper on Flooding Attack in MANET

Ruchita Meher, Seema Ladhe
Computer engineering, MGMCET kamothe Navi Mumbai, India
Computer engineering, MGMCET kamothe Navi Mumbai, India

Abstract
Mobile ad-hoc network (MANET) is widely applicable in various areas like military services, civilian environments and emergency operations. The issues in MANET are broadcasting, clustering, mobility management, bandwidth management and power management. Broadcasting becomes an important issue in MANET for route information discovery. The different routing attacks in MANET are flooding, black hole, link spoofing and wormhole attack. In this paper we are representing works proposed by various author on flooding attack. Our contribution in this paper is that we have presented details comparison of various counter based schemes.
Keywords: Broadcasting, Black hole, Flooding, MANET

I. Introduction

In Mobile ad-hoc network (MANET), each mobile terminal is an autonomous node. Hence, it worked as both host and router. MANET acts as light weighted terminal with less CPU processing capability, small memory size and less power storage. MANET does not provide centralized control. MANET distributes the control and management of the network among the nodes. Since the nodes are mobile, the network topology may change quickly and MANET acts as a dynamic network topology.

Since MANET allows the devices to maintain connection and also to add or remove the node from the network, it can easily used in the military battlefield to maintain the information network between the solider and vehicle as well as in commercial sector such as disaster relief effort for eg. Fire, flood or earthquake, etc. MANET is also used in personal area networking. MANET has some limitations like limited resources and physical security. It is also hard to detect the malicious node because of its volatile network topology.

There are some major issues involving in MANET such as broadcasting, clustering, mobility management, bandwidth management and power management. In this paper, we mainly focus on broadcasting since it involves the fluctuation of the signal strength and propagation with respect to time and environment. Due to mobile nature of nodes there is frequent change in topology which results in break of routing path hence broadcasting is used to discover neighbour and new path. For eg. Protocol such as AODV(Ad Hoc on Demand vector), DSR(Dynamic Source Routing), ZRP(Zone Routing protocol) and LAR(Location Aided Routing) use broadcasting to establish routes. Broadcasting in MANET is also important for providing the control and routing information for multicast and unicast protocol.

Broadcasting in MANET usually based on flooding in which source node sends a packet to its entire neighbourhood node. In broadcasting, each node receiving a broadcast packet and same will be simply re-transmits it to all its neighbours. Hence, we can say that broadcasting by flooding is usually very costly which results in serious transmission redundancy, contention and collisions in the network such a situation is referred to as the broadcast storm problem.

Various works on broadcasting has been done by many researchers. This paper gives the summary of all these work. Main contribution of this paper is we give detail comparison of various counter based schemes using neighbourhood information to achieve good performance in MANETs and reduce the broadcast storm problem.

II. Broadcasting in MANET

Broadcasting in MANET is the process where source node sends a message to all other node within its transmission radius. Sending a message to other hosts in the network is broadcast problem.

Broadcasting is spontaneous operation which can issue broadcast message at any time which result lack of synchronization and broadcasting is unreliable because there is no acknowledgement procedure as acknowledgement may cause additional contention.

Broadcast storm problem causes by flooding when a host receive broadcast message for the first time which has to be rebroadcasted but while rebroadcasting there should be following situation Redundant rebroadcast at the time to rebroadcast a broadcast message in mobile host already has the message.

Contention. At the same time the host will rebroadcast message to its neighbour then they contend with each other.
Collision. Collision is more likely to occur and cause more damage.

Broadcasting has many uses in MANET protocols such as finding a route to particular host using route discovery in routing protocols. E.g. MANET routing protocols such as Dynamic Source Routing (DSR), Ad Hoc on Demand Distance Vector (AODV), Zone Routing Protocol (ZRP), and Location Aided Routing (LAR) use broadcasting to establish routes. Following are the different Broadcasting schemes to solve broadcast storm problem are

Probabilistic scheme which rebroadcast packet with fixed probability p, Counter-based scheme which rebroadcast a number of received duplicate packets which is less than a threshold value, Distance-based scheme use distance between nodes to make the decision, Location-based scheme which gives location information of neighbors and Neighbor Based scheme which is a Cluster-based and selecting, forwarding neighbours.

III. Classification of MANET Protocol

Since MANETs has been in an active research area and in recent years many routing protocols have been introduced. A routing protocol specifies the communication which is carried out between the routers. The choice of that route selection is done by the routing algorithm. These main routing protocols are divided into 3 categories-

- Reactive protocols/On-demand
- Proactive protocols/Table driven
- Hybrid protocols

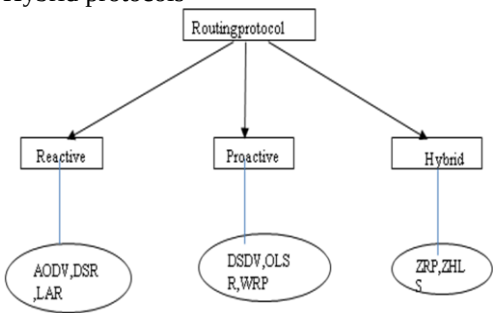


Fig1. Classification of MANET routing protocol

A. Reactive protocols

Reactive protocols also called as on demand driven protocols because they discover route only when it is on demand. It only establishes the route when source node in the network wants to send a message or a packet to destination node. The main thing of this protocol is that it reduces routing table when it is overflow but the bad thing is that longer delay has been seen as it is on demand The example of this type of protocol are DSR (dynamic source routing), AODV (ad hoc on demand distance vector routing), LAR (location aided routing), TORA (temporally ordered routing algorithm).

1. Ad-Hoc on Demand Distance Vector Protocol (AODV): AODV is commonly used reactive protocol in MANET. It establishes a route to a destination only on demand i,e node does not discover and maintain route until it demand. It is also a distance-vector routing protocol. AODV uses three main messages to determine a route they are RREQ, RREP, and RERR as follows:

Route Request Message (RREQ):

When a source node wants to communicate with another node, but does not have a route to reach that node Source node broadcasts a route request (RREQ) packet to all of its neighbors. The source creates an RREQ packet contains the source node IP address, current sequence number, destination IP address, last known destination sequence number , a broadcast ID , which is incremented with each RREQ and a Hop Count field.

Route Reply Message (RREP):

If a node receives an RREQ packet and it has a route to the target destination, then it unicast a route reply packet (RREP) to the neighbor that sent the RREQ packet. route reply message packet for the source include IP address , sequence number & hops to source and IP of neighbor from RREQ received

Route Error Message (RERR):

When the packet is not reached to the destination node or the link break happens then the host delete the route from the routing table and send the route error (RERR) message to the corresponding neighbors.

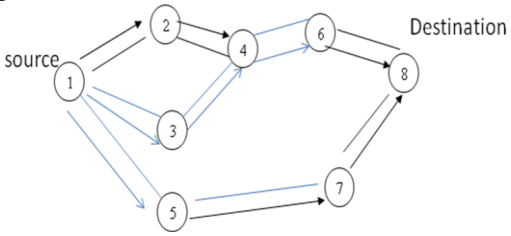


Fig 2. RREQ Packet

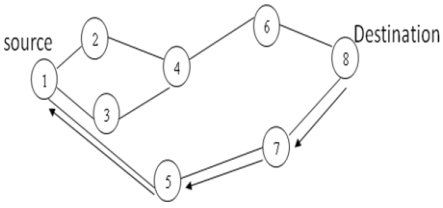


Fig.3 RREP Packet

*2. Dynamic source Routing (DSR):*It is a reactive protocol that generates a route on demand using source routing protocol. In Dynamic Source Routing, each source determines the route to be used in transmitting its packets to selected destinations. This protocol floods a route request message in the network to establish a route and there are two main components, called Route Discovery and Route Maintenance.

Route Discovery: Route Discovery determines the optimum path for a transmission between a given source and destination. It is an on-demand routing protocol, so to discover a route source node S need a route to destination node D first it broadcast RREQ packet then if Node A receive packet but has no route to D then it will rebroadcast packet by adding its address to source route then node C will receive RREQ but has no route to D again it will rebroadcast by adding address then Node D receive RREQ packet then it unicast RREP to Node C putting D in RREP source route as shown below:.

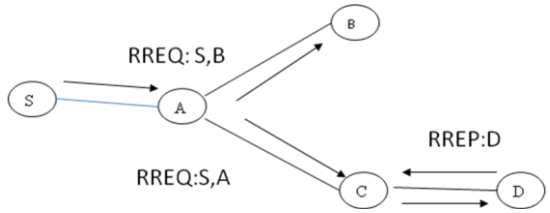


Fig. 4 Route discovery

Route Maintenance*:*

When communication starts, its responsibility of every node which is mentioned in the path that its next hop node should receive the data with path in the header

B.Proactive Protocol:

Proactive protocols are also called as table driven routing protocol because they maintain the routing table of the entire network. In proactive each node has to maintain its tables for storing routing information and also update the table i,e changes is done whenever the network changes. If any changes in topology as each node will send a broadcast message to entire network so it will affect the routing table for maintaining the routing entries. For large network proactive routing protocol not be suggested because for each node maintaining the table causes more bandwidth consumption and overload to routing table .the examples of proactive routing protocol are DSDV (destination sequence distance vector) and OLSR (optimised link state routing).

1. DSDV: The Destination-Sequenced Distance-Vector (DSDV) routing protocol based on the Bellman-Ford algorithm. In which each node maintains a routing table which stores next hop, destination and a sequence number that is created by the destination itself. In DSDV each node increment and add its sequence number periodically while forwarding routing table to its neighbors.

2. OLSR: The OLSR protocol is more efficient in networks with high density and high rarely traffic but the situation is when it is used in between a large number of hosts. OLSR requires that it continuously have some bandwidth in order to receive the topology updates messages.

C. Hybrid protocols

It is a combination of both reactive and proactive routing protocols. To overcome the weakness of reactive and proactive routing protocol the hybrid is mostly used. In hybrid routing protocol network is divided into zones. It is the most suitable routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state).

IV. Various Attacks in MANET

Attack in MANET can be classified as

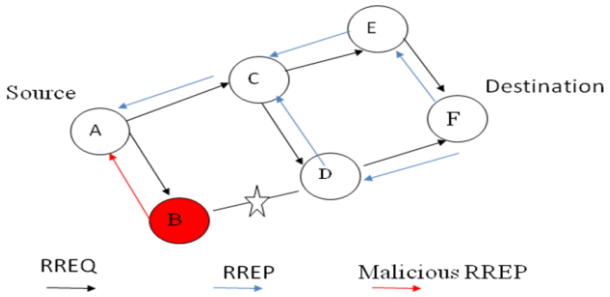
A. Active Attacks

Active attacks are the attacks in which attacker tries to disturb the performance of the network and also involves by modifying the data stream or creation of fake stream .Active attacks can be internal or external Internal Attack: Internal attack is from cooperate nodes which are actually part of the network.

External Attack: External attack carried out by node that does not belong to the domain of the network.

1. *Black hole attack:* The black hole attack is an active attack. It has two properties First is attacker sends fake routing information, declaring that it has the valid route from source to the destination, due to which other nodes in the network route the data packets through the malicious node. Second, malicious node targets the routing packets, drops them instead of normally forwarding them.

The Figure is an example of black hole attack in the mobile ad hoc networks was source node A and F represents the destination node. Node B is a misbehaviour node who replies the RREQ packet which is sent from source node, and makes a fake response that it has the shortest route to the destination node. Therefore source node incorrectly looks towards the route discovery process with completion, and starts to send data packets to node B. In the mobile ad hoc networks, a malicious node i,e node B probably drops the packets which is send by source node. So this misguiding node can be regarded as a black hole problem in MANETs.



Destinati
Fig 5 Black hole Attack [11]

2. Flooding attack: Flooding Attack can be begin by flooding the network with fake RREQ or data packet leading to the blocking of the network and reduces the probability of data transmission of the real node .Depending upon which type of packet used to flood in the network .it is classified into three categories are HELLO FLOODING,RREQ FLOODING And DATA FLOODING.

HELLO FLOODING: Some routing protocols in wireless network require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a range of the sender. Some misbehaving nodes in the network flood the Hello packet continuously. Without maintaining the hello interval. It creates the disturbances in the network operation. This activity diverts the legitimate node's action in the network. Figure 6 shows the hello flooding in the network.

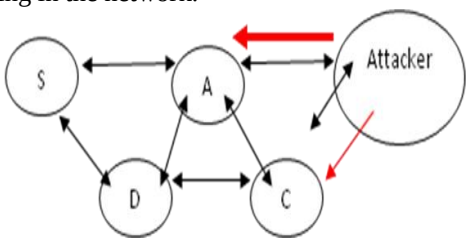
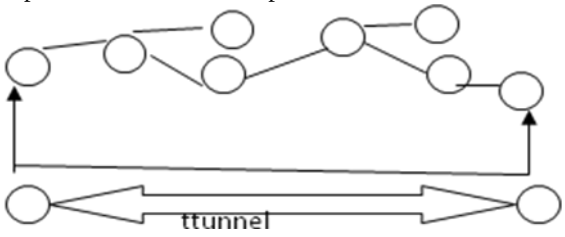


Fig 6 Hello Flooding attack [9]

RREQ FLOODING: In this type of flooding attack, the attacker broadcast many RREQ packets for the node which exist or not exist in the network. TO perform RREQ flooding the intruder disable the RREQ rate so it will effect on to consumes network Bandwidth.

DATA FLOODING: In Data flooding data packet are used to flood the network. In this flooding malicious node builds a path to all the nodes then send the large amount of fake data packet and this fake data packet fail the network resources so it will very hard to detect.

3. Wormhole Attack: In a wormhole attack, an attacker receives packets from one location in the network, tunnel" them to another location in the network, and then repeat them into the network from that location.. This tunnel between two colluding attacks is known as a wormhole In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used is not part of the actual network.



attacker attacker
Fig. 7 Wormhole attack [11]

4. Denial of service attack: The goal of a denial of service attack is to reject valid user's access to a particular resource. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

*5. Gray-hole attack:*This attack is also known as routing misbehaviour attack which show the way to dropping of messages. Gray hole attack has two phases .In the first phase the node itself advertise having a valid route to destination while in second phase, nodes drops interrupt packets within a certain probability As soon as it receive the packet from neighbor the attacker drop the packet.

6. Byzantine Attack: In this attack an intermediate node or a set of intermediate nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets on non – optimal path which results in degradation of the routing system.

7. Selfish Nodes: In this selfish node is not helping to communicate with other nodes which are taking part in the network. But malicious node which is not taking part in network operations, use the network for its advantage to save its own resources.

B. PASSIVE ATTACKS

A passive attack is an attack categorized by the attacker listening in on communication. In such an

attack, attacker does not try to break into the system or otherwise change data.

1. Traffic Monitoring: Traffic monitoring specifies for MANET and also other wireless network such as cellular, satellite and WLAN to developed or identify the communication and functional information for the launching of attacks.

2. Eavesdropping: The main goal of eavesdropping is to obtain some confidential information that should be secret during communication. This confidential information may include the location of public key or private key and also the password of the nodes

3. Traffic Analysis: Traffic analysis is a passive attack used to increase the information from which node can communicate with each other and also how data should process.

V. Various Approaches Used To Overcome From Broadcast Storm Problem (Flooding Attack)

A. CBS: Counter-based broadcast Scheme in Mobile ad hoc networks. [3]

A counter based scheme has been suggested to reduce the redundant rebroadcast and alleviating broadcast storm problem..This research proposes counter based algorithm that dynamically adjust the counter threshold value using neighbourhood information Counter based scheme is one of the broadcasting technique in MANET. In CBS when we receiving a message a counter *c* is set to keep track of number of duplicate messages received, counter threshold C is chosen and Random Assessment Delay (RAD) timer is set. Initially set counter c as1.When the RAD timer expires the counter is tested against a fixed threshold value *C*, if counter is greater than or equal to threshold C then the broadcasting should stop otherwise proceed.

This method gives fixed threshold value so it scores high efficiency only when used with uniform density networks; when the network is sparse a high threshold is used and when dense low threshold value

B. ACBS: Adaptive counter-based Scheme in Mobile Ad hoc network [4]

As we know that threshold value is based on local connectivity information so when topology of MANET change Individual host can also changes so it dynamically adjust own threshold value based on its neighbour status. So it extends fixed threshold c into function Threshold = C(n) where n is the number of neighbors . The function C(n) is undefined yet. In this paper we have extend threshold value. Adaptive counter-based scheme uses the extended fixed threshold C into a function C(n), where n is the number of neighbours of the host. Thus, each host will use a threshold C(n) depending on its current value of n it determine whether to rebroadcast or not. The Execution of the algorithm is same as that of fixed counter based only we will check the counter value c with C(n) i,e if counter c is less than C(n) then it resume for rebroadcast otherwise cancel the transmission.

This method only maintain the records of a packet rebroadcast status packet for every node by considering threshold value but node can be in sparse or dense network this situation is not considered in this paper.

C. NCBS: New Counter Based Broadcast scheme in Mobile ad-hoc network [5]

The New Counter-Based (NCB) uses the average number of neighbour to dynamically adjust the threshold value to adjust in either sparse or dense network. The Algorithm is based on a counter c that is used to keep track of the number of times the broadcast packet is received. A counter threshold is decided based on neighbouring information.. Whenever c is greater than or equal to the threshold, the rebroadcast is inhibited. It dynamically adjusts the counter based threshold value c at each mobile host according to the value of the local number of neighbours. The value of c changes when the host moves to a different neighbourhood. In a sparser area, the counter based threshold value c is smaller and in denser area, the counter based threshold value c is larger. We present an estimate of average neighbour number as the basis for the selection of the value of c. Let A be the area of an ad hoc network, N be the number of mobile hosts in the network, and R be the transmutation range. The average number of neighbour n'can be obtained

$$n' = (N-1)0.8*\Pi^2/A$$

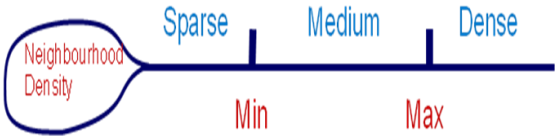
In addition, when integrated in the Ad hoc On-Demand Distance Vector (AODV) routing protocol, NCB will perform better than both standard and fixed counter-based AODV protocols. In this method Only average no. of nodes can consider which can not be sufficient for rebroadcasting.

[10]

D. HACB: Highly Adjusted Counter-Based Broadcast scheme in MANET [6]

The Highly Adjusted Counter-Based (HACB) uses three items of derived neighbourhood information the maximum, the minimum in addition to the average number of neighbours to dynamically adjust the threshold value. HACB is better than ACB

however, perhaps with an added complexity. In HACB algorithm based on counter c that is used to keep track of no. of times the broadcast packet is received, A counter threshold decided based on neighbouring information that is in sparse network threshold is c1 and for medium and dense threshold value is c2 and c3 respectively. In this algorithm we are considering the min threshold value n1and maximum threshold value n2 so by comparing the no. of neighbour (n) to minvalue n1. If(n<n1) then network is in sparse area else if it is in between n1 and n2 then network is in medium area else if(n>n2) then the network is in dense area so from this algorithm we are rebroadcasting no. of packet in particular area to form a route. Min and Max value are not specified so exact no. of neighbour cannot be concluded and also No acknowledgement from nodes while receiving packet from the node.



[10]

E. Dynamic Probabilistic Counter-Based Scheme in MANET[7]

DPCBS is the Combination of counter based and probability based broadcasting scheme. In DPCBS we first initiate a counter c that records the number of times a node receives the same packet. Such a counter should maintained by each node for each broadcast packet. After waiting for a random assessment delay (RAD) time which is randomly chosen from a uniform distribution between 0 and Tmax seconds, where Tmax is the highest possible delay interval, if c reaches a predefined threshold C, the packet is rebroadcast with a low rebroadcast probability P1 (the node is in dense area). Otherwise, the packet is rebroadcast with a high rebroadcast probability P2 (where P1 < P2, and therefore the node is in sparse area). DPCBS adjusts the forwarding probability dynamically by the use of the function f(c) which is defined

$$F(c) = \{ e^{-(c/C)} \quad ; \quad c<=C$$
$$` F(c) = \{e^{-(c+1/C)} \quad ; \quad \text{otherwise}$$

In this method we are investigating the performance of these broadcasting algorithms in real applications, such as route discovery process is lacking. As we are calculating the probability but exactly no. of nodes to be rebroadcast is still missing it which gives the possibility value.

F. PCB: Position-aware counter-based broadcast for MANET [8]

It is a combination of position based and counter-based schemes. In PCB, each node is able to make a local decision about whether to rebroadcast, according to its adaptive EAC threshold and counter threshold. whenever a node rebroadcasts a packet it adds its own GPS address (X, Y, Z) to the header of the packet. When a node receives a packet, it notes the location of the sender and calculates EAC. Here we introduce a new mechanism of two-tier threshold of EAC. That is if the EAC is less than the first tier threshold value Vth1, the node will not rebroadcast, and all future the same packet will be ignored. Otherwise, compare EAC with the second tier threshold value Vth2 to assign an appropriate RAD to the node before delivery. At the same time, initiate a counter C to one. The EAC calculation and threshold comparison occur with all redundant broadcasts received before its RAD expires. Increase C by 1 only when calculated EAC of packet is larger than Vth1. When the RAD expires the counter is checked against the threshold value Cth (Ch or Cl which is set differently from one node for a given EAC. If the counter is less than or equal to the threshold, the packet is rebroadcast. Otherwise, it is simply dropped.

In this method we are calculating the EAC of node and from that we are getting the transmission range of a node to rebroadcast a packet but not exactly the no. of nodes. It demands accurate neighbourhood information and cannot ensure the coverage with outdated topology information

VI. Comparison Of Various Counter Based Broadcast Scheme

In this section table summarizes the brief comparison between various counter based broadcasting schemes on the basis of parameters like counter methods, tool used, its Reachability, Saving rebroadcast and its drawback.

Table 1 Summary of various counter based broadcast scheme

Paper	Method	Tools Used	Reach ability [RE]	Saving Rebroadcast	Drawback
counter-based scheme[3]	RAD timer	NO	RE will be poor	Threshold is larger value SR degrade	Threshold is constant
Adaptive counter-based Scheme[4]	Threshold = C(n)	NO	RE is always at high level	SR is significant	Neighbourhood density sparse and dense area is not considered
New Counter Based Broadcast scheme[5]	Average no. of nodes	NO	RE will be poor	Threshold is large redundant rebroadcasts will be generated.	Average no. of nodes cannot be sufficient for finding neighbour
Highly Adjusted Counter-Based (HACB) Broadcast[6]	Max and Min no. of neighbours	NO	(T*r/)100	(r-t)/r	Min and Max values are not specified for finding neighbour
DP Counter Based Scheme [7]	Combination of probability based and counter based	NO	(T*r/)100	(r-t)/r	Probability is calculated but nodes to be rebroadcast will not gives the possibility value.
PCB broadcast Scheme[8]	Combination of counter based and position based	GPS	r/e	(r-t)/r	. High number of control messages exchanged to broadcast one packet coverage

T-total no. of nodes, r-no. of receive node , e- no. of reachable node, t- no. of host transmit packet

VII. Conclusion

In this paper we focus on various approaches to overcome flooding attack using different counter based broadcasting scheme. These schemes are effective for developing appropriate threshold value so that node will rebroadcast packet to its neighbours and form a route and also increases the reachability, save rebroadcasting and average latency. The result of our implementation show better impact to overcome flooding attack.

References

[1] Y.-C. Tseng, S.-Y. Ni, and E.-Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop ad hoc networks", IEEE TRANSACTION ON COMPUTERS, VOL. 52, PP. 545-557, 2003.

[2] Wei Lo and Jie Wu, "On Reducing Broadcast Redundancy in Ad Hoc Wireless Networks". IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 1, NO. 2, APRIL-JUNE 2002.

[3] B. Williams, T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks".(MOBIHOC 2002).PROCEDING OF ACM INTERNATIONAL SYMPOSIUM ON MOBILE AD-HOC NETWORKING. PP.194-205,2002.

[4] Y.-C. Tseng, S.-Y. Ni, and E.-Y. Shih, "Adaptive Approaches to Relieving Broadcast Storms in a wireless multihop mobile ad hoc network". IEEE TRANSACTIONS ON COMPUTERS, VOLUME52 (5),PAGES 545-557,MAY 2003..

[5] M. Bani yassein, S. Al-Humoud, M. Ould Khaoua and L. M. Mackenzie, "New Counter based Broadcast Scheme using local Neighborhood Information in MANETs."
[6] M. Bani yassein, A. Al-Dubai, M. Ould Khaoua, Omar M. Al-jarrah, "New Adaptive counter based Broadcast Using Neighborhood Information in MANET's"., IEEE 2009.
[7] M, M. Khaoua, "Dynamic Probablistic Counterbased Broadcasting in MANET",IEEE 2010.
[8] Xiaoman Wu, Yilan Yang, JieLiu, Yue Wu, Fasheng Yi, "Position-aware counter-based broadcast for MANET's." IEEE 2010.
[9] The Network Simulator ns-2,http://www.isi.edu/nsnam/ns/ns-man.html
[10] Q. Zhang and D. P. Agrawal, "Dynamic Probabilistic Broadcasting in MANETs," JOURNAL OF PARALLEL AND DISTRIBUTED COMPUTING, VOL. 65,PP. 220-233, 2005.