# Secured System against DDoS Attack in Mobile Adhoc Network

ARUNMOZHI ANNAMALAI, VENKATARAMANI YEGNANARAYANAN
Department of Electronics and Communication Engineering
Saranathan College of Engineering, Trichy
India
saarunmozhi@gmail.com http://www.saranathan.ac.in

*Abstract:* - The risks to users of wireless technology have increased as the service has become more popular. Due to the dynamically changing topology, open environment and lack of centralized security infrastructure, a mobile ad hoc network (MANET) is vulnerable to the presence of malicious nodes and to ad hoc routing attacks. There are a wide variety of routing attacks that target the weakness of MANETs. This paper focuses on mobile ad hoc network's routing vulnerability and analyzes the network performance under two types of attacks, flooding attack and black hole attack that can easily be employed against the MANETS. The resistive schemes against these attacks were proposed for Ad hoc on demand Distance Vector (AODV) routing protocol and the effectiveness of the schemes is validated using NS2 simulations.

*Key-Words:* - **S**ecurity, Defense, Mobile adhoc network, Denial of service, Flooding attack, Black hole attack

## 1 Introduction

A MANET is a self-configuring network of mobile devices connected by links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. There are generally two types of ad hoc routing protocols, reactive and proactive routing protocols. The focus of this paper centres on reactive routing protocols which establish routes between communicating nodes when needed using a route discovery process involving Route Requests and Route Replies, a process which can be easily misused for denial-of-service attacks. The type of security attack in MANET is denial of service attack (DoS). A DoS attack is an attempt to prevent legitimate users of a service or network resource from accessing that service or resource. A Distributed Denial-Of-Service (DDoS) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated.

The networks are particularly vulnerable to DoS attacks launched through compromised nodes or intruders. The intruder broadcasts mass Route Request packets or sends a lot of attacking DATA packets to exhaust the communication bandwidth and node resources so that the valid communication cannot be kept. In this paper, we have analyzed two types of attacks namely flooding attack and black hole attack in detail. The resisting mechanisms over these attacks are proposed and the effectiveness of the proposed schemes is validated with simulations.

## 2 Security Attacks on MANETS

The main security services for MANETs are authentication, confidentiality, integrity, non-repudiation and availability. Authentication means that correct identity is known to communicating partner; confidentiality means certain message information is kept secure from unauthorized party; integrity means message is unaltered during the communication; nonrepudiation means the origin of a message cannot deny having sent the message; availability means the normal service provision in face of all kinds of attacks.

Attacks on MANETs come in many varieties and they can be classified based on different aspects. According to the legitimate status of a node, an attack could be external or internal. The external attacks are committed by nodes that are not legal members of the network, while the internal attacks are from a compromised member inside the network. The internal attacks are not easy to prevent or detect. These attackers are aware of the security strategies, and are even protected by them. The internal attacks pose a higher threat to the network. In terms of interaction, an attack could be passive or

active. Passive attacks do not disrupt the communication. Instead, they intercept and capture the packets to read the information. On the other hand, active attackers inject packets into the network to interfere or interrupt the network communication, overload the network traffic; fake the legitimate node or package, obstruct the operation or cut off certain nodes from their neighbours so they cannot use the network services effectively anymore.

Attacks could also be classified according to the target layer in the protocol stack. By targeting the physical layer of a wireless network or a wireless node, an attacker can easily intercept and read the message contents from open radio signals. An attacker can jam or interfere the communication by generating powerful transmissions to overwhelm the target signals. The jamming signals do not follow the protocol definition, and they can be meaningless random noise and pulse. By targeting the link layer, an attacker can generate meaningless random packets to grab the channel and cause collisions. In this situation, if the impacted node keeps trying to resend the packet, it will exhaust its power supply; the attacker can passively eavesdrop on the link layer packets; the link layer security protocol WEP is vulnerable too, the initialization vector (IV) flaw in the WEP protocol makes it easier for an attacker to launch a cryptanalytic type attack. Coming along with many new routing protocols introduced to the MANETs, many new types of attacks were presented to target these specific protocols. By targeting the transport layer, a desynchronization attacker can break an existing connection between two nodes by sending fabricated packets exceeding the sequence number to either node of the connection. It may result in letting the node keep sending retransmission requests for the missed frames.

By targeting on the application layer, a Repudiation attack is a threat to a business that relies on electronic traffic. Other application layer attacks, such as viruses, worms, trojans, spywares, backdoor, and data corruption or deletion, target either application layer protocols, such as FTP, HTTP, and SMTP, or applications and data files on the victims.

Some attacks target security leaks on the cryptography primitive of the protocols. Digital signature attacks target RSA public-key encryption algorithms. Attackers forge the message signature based on the signature of a legitimate message. Digital signature attacks have three types, known-message, chosen message, and key only attacks. The Known-message attacker knows a list of messages previously signed by the victim. The Chosen-message attacker can choose a specific message that it wants the victim to sign. The Key only attacker knows the public verification algorithm only.

Hash collision attacks target hash algorithms, such as SHA-1, MD4, MD5, HAVAL-128, and RIPEMD, to construct a valid certificate corresponding to the hash collision. Pseudorandom number attacks reverse engineer the pseudorandom number generators used by the public key mechanisms to break the cryptography.

# 3 Background

Routing in MANETs is difficult since mobility causes frequent network topology changes and requires more robust and flexible mechanisms to search for and maintain routes. When the network nodes move, the established paths may break and the routing protocols must dynamically search for other feasible routes. Many protocols have been proposed for MANETs. These protocols can be mainly divided into two categories as proactive and reactive protocols.

Proactive Routing Protocols maintain routes to all destinations, regardless of whether or not these routes are needed. In order to maintain correct route information, a node must periodically send control messages. Therefore, proactive routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no data traffic. The main disadvantages of such algorithms are respective amount of data for maintenance and slow reaction on restructuring and failures. The main advantage of this category of protocols is that hosts can quickly obtain route information and quickly establish a session. DSDV, OLSR and CGSR are some of the well known proactive routing protocols for MANETs. Reactive protocols do not execute a routing update until the communication needs it. When a route is needed, the source node initiates a route discovery process to the destination. Once established, the route must be maintained until it is no longer needed or the destination node becomes inaccessible. Reactive routing protocols can dramatically reduce routing overhead because they do not need to search for and maintain the routes on which there is no data traffic. This property is very appealing in the resource-limited environment. AODV, DSR and TORA are some of the well known reactive protocols for MANETs.

The AODV Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing

control messages. AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. When the source node wants to make a connection with the destination node, it broadcasts a RREQ message. This RREQ message is propagated from the source, received by neighbours (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbours. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value.

# 4 Flooding Attack

## 4.1 RREQ Flooding Attack

Reactive routing protocols like AODV and DSR, used in MANETs, flood the network with route requests whenever a new route is to be discovered. This technique of flooding can be easily misused by malicious nodes to disrupt the network. Generally all nodes have a limit beyond which requests cannot be sent. Malicious nodes can easily bypass this limit and send out large numbers of fabricated route requests in the network. Flooding RREQ packets in the whole network will consume a lot of resource of network. To reduce congestion in a network, the AODV protocol adopts some methods. A node can not originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value. Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential backoff. The first time a source node broadcasts a RREQ, it waits roundtrip time for the reception of a RREP. If a RREP is not received within that time, the source node sends a new RREQ. When calculating the time to wait for the RREP after sending the second RREQ, the source node MUST use a binary exponential backoff. Hence, the waiting time for the RREP corresponding to the second RREQ is 2 * round-trip time. The RREQ packets are broadcast in an incrementing ring to reduce the overhead caused by flooding the whole network.

In the Ad Hoc Flooding Attack [10], the attack node violates the above rules to exhaust the network resource. The attacker tries to send excessive RREQ without considering RREQ_RATELIMIT within per second. The attacker will resend the RREQ packets without waiting for the RREP or round-trip time. In the Flooding Attacks, the whole network will be full of RREQ packets which the attacker sends. The communication bandwidth is exhausted by the flooded RREQ packets and the resource of nodes is exhausted at the same time. For example, the storage of route table is limited. If mass RREQ packets are coming to the node in a little time, the storage of route table in the node will exhaust so that the node cannot receive new RREQ packet. As a result, the legitimate nodes cannot set up paths to send data.

## 4.2 Data Flooding Attack

When nodes in MANET find the correct routing path, source nodes send the data packets through that route. In data flooding attack, the attacker first maintains the routes to destination node, then sends frequently the useless data packets. The destination node will then be engaged in receiving the excessive data packets from the attacker and cannot work properly. The attacker packets engage the network and stop the processing of legitimate data packets.

# 5 Black hole Attack

A black hole attack is a type of denial of service attack accomplished by dropping packets. In black

hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocols based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is established, now the attacker node may drop all the packets or forward it to the unknown address. To succeed in the black hole attack, the attacker must generate its RREP with destination sequence number greater than the destination sequence number of the destination node. It is possible for the attacker to find out destination sequence number of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's destination sequence number based on the received RREQ's destination sequence number.

# 6 Proposed Work

## 6.1 Defense Scheme against flooding Attack

The defense against RREQ flooding and data flooding attack are performed with the help of algorithm I and algorithm II.

The RREQ flooding attacker will not follow the binary exponential backoff which is normally adopted by the RREQ of AODV scheme. In this proposed scheme, 2 steps are carried out for resisting the RREQ flooding attack. In the first step, each neighbouring node checks the time to wait for the RREP follows the binary exponential backoff. The nodes which do not obey this backoff are identified as the suspicious node. The nodes then perform the second step of defense scheme. In this second step, the RREQ rate is checked. Here, we maintain two threshold values. The RREQ_RATELIMIT is considered as the upper threshold (UT) and RREQ_RATELIMIT /2 is taken as lower threshold (LT). If RREQ rate is less than LT, the node which forwards the RREQ is identified as the normal node. If the RREQ rate lies between LT and UT, the forwarding node is identified as the suspicious node. The RREQ is then delayed in a queue. If RREQ rate is above UT, the forwarding node is identified as the attacker and the RREQ are dropped. The attacking node ID is broadcast to all nodes in the network. Hence, the attacking node is isolated from the network.

To resist the data flooding, in this paper, we propose a new defense mechanism that maintains the flow Information monitoring table (FIMT). It contains flow id, source id, packet sending rate and destination id. Sending rates are estimated for each flow in the intermediate nodes. The updated flow information is sent to the destination along with each flow. The destination node sends the control message to notify the sender nodes about the congestion. The sender nodes, upon seeing these packets, will then reduce their sending rate. If the channel continues to be congested because some sender nodes do not reduce their sending rate, it can be found by the destination using the updated flow details. It checks the previous sending rate of a flow with its current sending rate. When both rates are same, the corresponding sender of the flow is identified as an attacker. Once the DDoS attackers are identified, all the packets from those nodes will be discarded. The attacker is blocked from the communication. Hence network resources are made available to the legitimate nodes in the network.

Since the proposed scheme maintains state for traffic streams traversing node x on an in-hop/out-hop basis, it is a stateful protocol. Let i and j denote one-hop neighbours of the node x. An entry for flow information is maintained for each pair (i, j). An in-out stream corresponding to (i, j), is the traffic generated by a set of flows crossing the sub-path (i, x, j). For each in-out stream which crosses the node x, a record of the traffic rate is maintained by the node x. If the number of neighbours of the given node x is N, then by the number of active in-out streams, the total number of entries is estimated as $N(N-1)$. The $(i, j)^{th}$ entry in the FIMT maintains the assigned rate ARij for the in-out stream (i, j), the counter $C_{ij}$ for the number of bits received in the current measurement window and the measured rate $MR_{ij}$ for the previous measurement window. Each FIMT node regulates the in-out stream (i, j) to the assigned rate $AR_{ij}$ by using the measured rate $MR_{ij}$. The Distributed rate control process is used for rate controlling in our proposed scheme.

### 6.1.1 Algorithm I

1. Each neighboring node checks the time to wait for the RREP follows the binary exponential backoff.
2. If backoff is not satisfied go to step 4.1.
3. Else if
   3.1. RREQ_RATELIMIT = UT,
   3.2. RREQ_RATELIMIT/2 = LT.

3.3. RREQ rate < LT

Identify the node which forwards this RREQ packet as Normal Node

4. Else RREQ rate < UT
   4.1 Identify the forwarding node as the Suspicious Node (SN).
   4.2 RREQ packet is delayed in a queue.
5. Else
   Identify the node as Attacking Node (AN).
6. Endif
7. AN is blocked from the network.

#### 6.1.2 Algorithm II

1. Different flows are transmitted from different sources to destinations.
2. FIMT stores the information of each flow.
3. From FIMT, the assigned rate $AR_{ij}$ is calculated for each flow.
4. Intermediate nodes send updated FIMT of all flows to destination.
5. If congestion is detected, distributed rate control is applied and the actual rate of each flow is assigned as $ACR_{ij}$
6. At the time interval T, the measured data rate is noted.
7. if $MR_{ij} > ACR_{ij}$, then
   7.1. Source status = REJECTED
   7.2. Attacker address = Source IP address
8. End if
9. If source status = REJECTED, then
   9.1 Remove the node from the list.
   9.2 Block all the traffic from the attacker
10. End if.

### 6.2 Defense Scheme Against Black hole Attack

To resist the black hole attack, we propose a defense mechanism which could be potentially exploited by malicious nodes. A Neighbourhood Route Monitoring Table (NRMT) is maintained by each node in the network. The NRMT maintains packet routing information of its neighbour nodes. It contains the source ID, destination ID, source sequence number, destination sequence number, and a threshold value of sequence number which is dynamically updated, the time at which RREQ packet enters the node (RREQ-IN-TIME), the time at which RREQ packet leaves the node (RREQ-OUT-TIME), the time at which RREP packet enters the node (RREP-IN-TIME) and the time at which RREP packet leaves the node (RREP-OUT-TIME).

If the node is the normal node, once it receives the RREQ packet, it checks its routing table to identify whether it is the destination or not. According to AODV protocol, if it is the destination node, it will send the RREP packet to the source node through its route or it will forward the RREQ to its one hop neighbour. Checking the routing information from the table requires a minimum time period known as MIN-TIME. If the node is the black hole node, it will send a RREP message without checking the table. The NRMT maintains the record of the time of Reply.

The first step of the detection process is based on the timing information of NRMT. Every node in the network when it receives the RREP from its neighbour, finds DIFF-TIME which is the difference between the RREQ-OUT-TIME and RREP-IN-TIME and compares this with MIN-TIME. If the RREP is from the black hole node DIFF-TIME will be less than the MIN-TIME. The node is identified as a suspicious node.

It is well known that the black hole node assigns a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. As the second step of detection mechanism, RREPs sequence number is compared with the threshold value of sequence number. In this protocol, the threshold value is dynamically updated at every time interval. If the current sequence number is greater than the threshold value the node is confirmed as black hole and it is eliminated from the routing table. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources.

## 7 Simulation and Results

The network simulator ns2 is used to simulate the experiment. The parameter settings for the simulations are: the radio propagation mode is Two Ray Ground, antenna type is Omni antenna, interface queue length is 50 (packets), queue management scheme is Drop Tail, routing protocol is AODV, height of antenna is 1.5m, transmission distance is 250m, signal interference or sensing distance is 550m. The speed of the mobile node is 10m/s. The simulated traffic is Constant Bit Rate (CBR). The network covers the simulated area of 1200m x 1200m.

### 7.1 Simulation Implementation and Evaluation for flooding attack

The performance of our proposed scheme against RREQ flooding attack is analyzed for MANET with and without defence scheme. The protocol was implemented and evaluated in the ns-2 network simulation environment. Number of nodes is a varying parameter as it plays important role in network performance. The packet delivery ratio is the ratio of the number of packets received successfully to the total number of packets sent. Fig. 1 shows how the packet delivery ratio (PDR) is varied by varying the number of nodes to account for system scalability. It is seen that the PDR was improved up to 76.9% when our protocol was implemented. The pause time was also varied and the PDR was obtained. Pause time can be defined as time for which nodes waits on a destination before moving to other destination. Low pause time means node will wait for less time thus giving rise to high mobility scenario. Our simulations from Fig. 2 show how PDR is varied by varying the pause time of a node in the network. It is clear that PDR increases as pause time increases. This is because low mobility allows more stable routing paths. However, it is not possible to achieve 100% packet delivery due to the unreliable links in wireless networks.

Fig.3 and Fig. 4 show the performance of our proposed work against data flooding attack. All the source nodes negotiate a rate of 100 kbps for traffic flow and begin sending traffic on flow at a rate of 100 kbps at time t = 1.0 sec. The attacking flow is set at a rate of 500 kbps. The capacity of the link is set to 2 Mbps. It is seen that PDR is much improved with our proposed scheme. Our protocol confirms the ability to provide resistance against data flooding attacks.

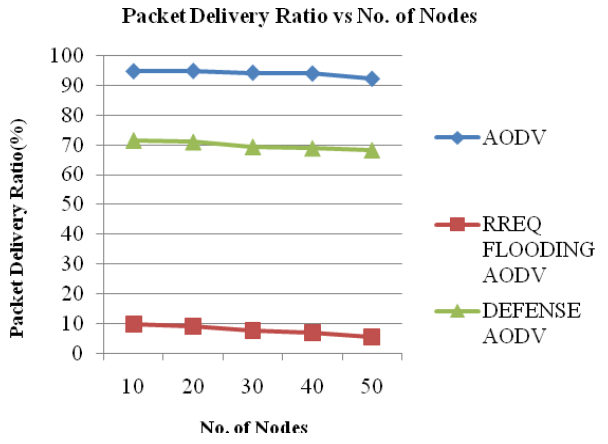


Fig.1 Impact of defense scheme against RREQ flooding attack with varying number of nodes

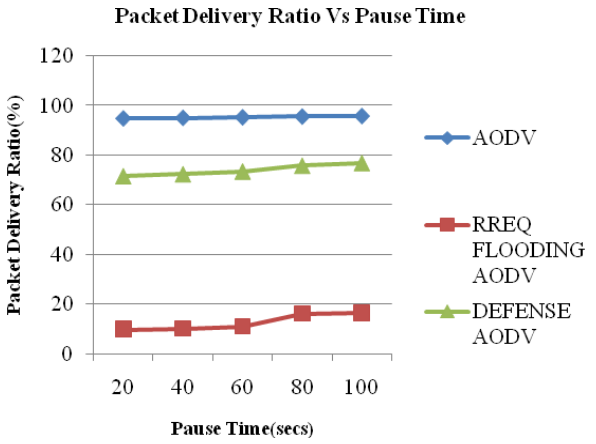


Fig.2 Impact of defense scheme against RREQ flooding attack with varying pause time.

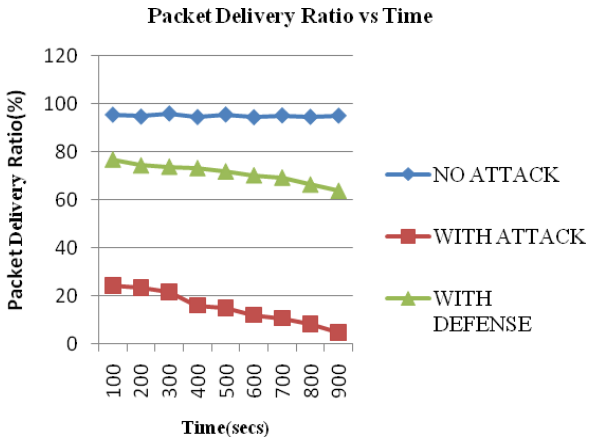


Fig.3 Impact of defense scheme against data flooding attack with simulation time

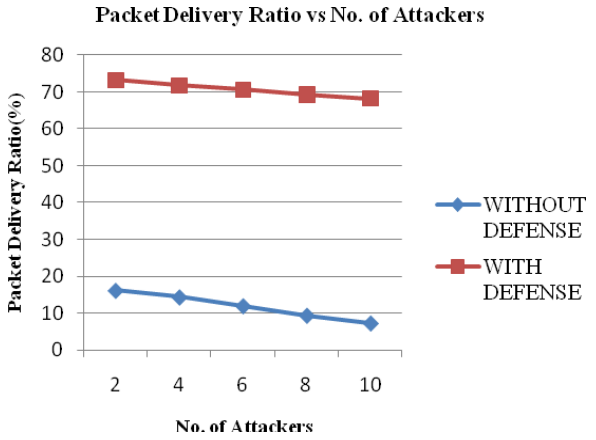


Fig.4 Impact of defense scheme against data flooding attack with varying number of attackers

### 7.2 Simulation Implementation and Evaluation for black hole attack

To defend against the black hole attack in MANET, the NRMT protocol was implemented and evaluated in the ns-2 network simulation environment. We have implemented the simulation of MANET with 2 different cases. In the first case, we have established 2 UDP traffic flows with the data rate of 50kbps and the packet size of 512 bytes. We have implemented an AODV protocol that simulates the behaviour of a black hole and we simulated 50 scenarios each involving different ad-hoc networks with 30 nodes each moving randomly. We have introduced a black hole in each scenario and compared the performance of the networks with and without a black hole. We then implemented the NRMT method to detect and discard the black hole node.

The performance of the network is evaluated based on the packet delivery ratio. The effect of black hole attack in AODV and the effect of NRMT method are observed from Fig. 5. Since the black hole attack is effectively detected based on NRMT, it can be informed to all the other nodes in the network immediately. Hence the attack is removed easily from the network. This follows that the number of successfully received packets get increased and it improves the packet delivery ratio. However, the packet delivery ratio for the AODV protocol without attack will be more for any number of nodes in the network.

The average end-to-end delay calculates the delay of all the packets that have been successfully transmitted from the source to the destination. It includes all possible delays caused by buffering during route discovery latency, queuing in the interface queue, retransmission delays at the MAC, propagation, and transfer times. In the proposed scheme we have adopted the 2 step procedure to detect the attack. Hence the average end to end delay for the NRMT scheme is greater than the other two cases. The effect of average end to end delay is shown in Fig.6.

The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. The routing load metric evaluates the efficiency of the routing protocol. The routing overhead is also evaluated with varying number of nodes. The overhead with the defense scheme is greater than the black hole attack case. This is because of the control packets that are sent to the nodes in the network by the node which detects the black hole. But the routing overhead required for NRMT method is less than that required for the AODV protocol without attack. The effects of routing overhead are shown in Fig. 7.

In the second case of simulation the number of UDP flows is varied. The packet delivery ratio, average end to end delay and routing overhead are evaluated. The impact is shown from Fig. 8 to Fig. 10. It is observed that the proposed scheme gives better packet delivery ratio than the black hole attack case. But the average end to end delay and the routing overhead are greater than the black hole attack case.

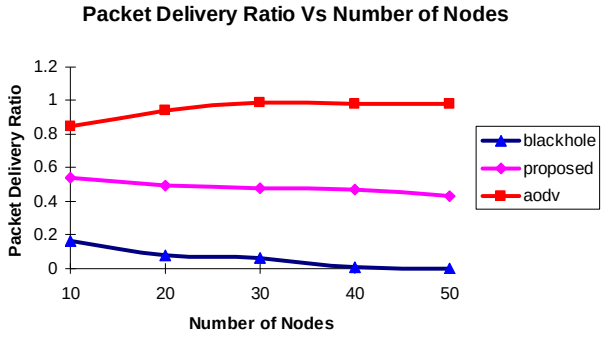


Fig.5 Impact of Packet Delivery Ratio with varying No. of Nodes

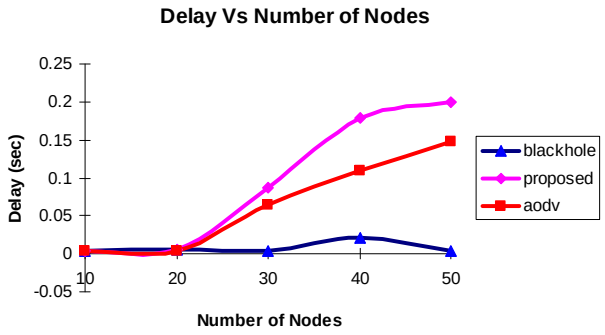


Fig. 6 Impact of Average End to End Delay with varying No. of Nodes

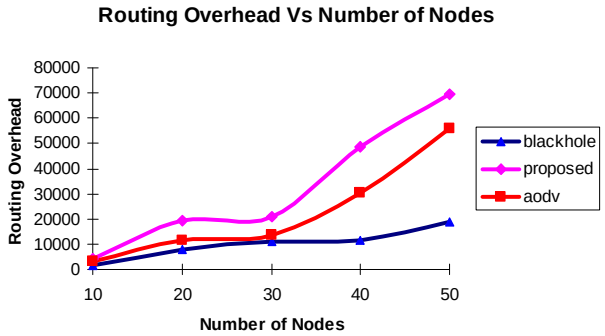


Fig. 7 Impact of Routing Overhead with varying No. of Nodes

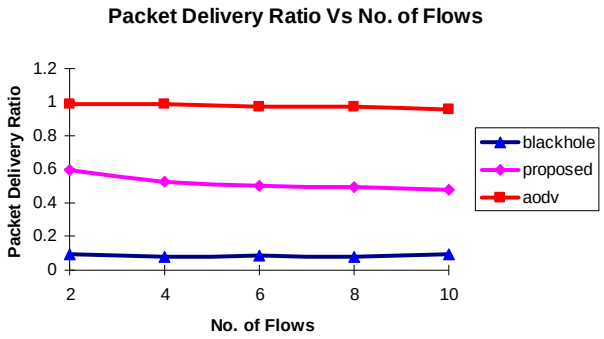


Fig. 8 Impact of Packet Delivery Ratio with varying No. of Flows

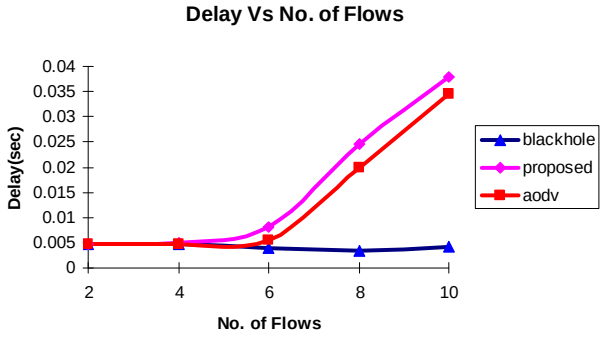


Fig. 9 Impact of Average End to End Delay with varying No. of Flows

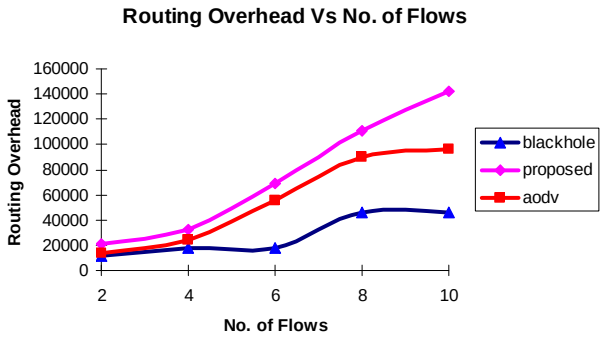


Fig. 10 Impact of Routing Overhead with varying No. of Flows

## 8 Related Work

Arunmozhi S.A. and Venkataramani Y. [1] have proposed the Flow Monitoring (FMON) scheme for MANETs that is resistant to the Reduction of Quality (RoQ) attack. RoQ attack is a new style of DDoS attack which is difficult to detect. RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems gradually rather than refusing the clients from the services completely. The FMON protocol employs MAC layer-based detection scheme and a response scheme based on Explicit Congestion Notification (ECN) marking. The scheme requires each node to maintain state information for each aggregate in out traffic stream traversing an input-output pair, as opposed to every flow, thus making the scheme more scalable. Each node performs rate monitoring/adjustment functions on each in out stream to prevent DoS conditions. When a node experiences congestion due to attack flow, ECN mechanism helps the legitimate sender to reduce the sending rate. If the channel continues to be congested, updated FMON helps to detect the attackers and reject the attacking flows. This makes the network resources available to the legitimate users. FMON protocol confirms the ability to provide resistance against RoQ DDoS attacks.

Jelena Mirkovic and Peter Reiher [2] have proposed a source-end DDoS defense system that achieves autonomous attack detection and adaptive response at the source-end. Ping Yi et al. [3] have developed Flooding Attack Prevention (FAP), a generic defense against the Ad Hoc Flooding Attack in mobile ad hoc networks. The FAP is composed of neighbour suppression and path cutoff. When the intruder broadcasts exceeding packets of Route Request, the immediate neighbours of the intruder observe a high rate of Route Request and then they lower the corresponding priority according to the rate of incoming queries. Ming-Yang Su [7] has proposed several intrusion detection system (IDS) nodes which are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. Supranamaya Ranjan et al. [8] have proposed a counter-mechanism called DDoS Shield against DDoS attack that consists of a suspicion assignment mechanism and a DDoS-resilient scheduler. Zhiqiang GAO and Zhiqiang [15] have proposed a technique to defend against distributed denial of service attacks based on TCP. It uses proactive tests to identify and isolate the malicious traffic. Elmar Gerhards-Padilla et al. [17] proposed a centralised approach, using topology graphs to identify nodes attempting to create a black hole. It performs plausibility checks of the routing information propagated by the nodes in the network. An alarm is triggered if the plausibility check fails.

# 9 Conclusion

Security is an important feature for wide deployment of MANET. A variety of attacks have been discussed. In this paper, we have analyzed two types of DDoS attacks such as flooding attack and black hole attack. Defense scheme against RREQ flooding attack based on binary exponential backoff and RREQ_RATELIMIT was proposed. For resisting the data flooding attack, a FIMT scheme was developed based on the flow information. The attackers are effectively identified with the proposed scheme. We have also described the black hole attack that can be mounted against a MANET, and proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevented the network form further malicious behaviour. We have developed a NRMT scheme for MANETs that is resistant to the black hole attack. The scheme identifies the attacker based on timing information and destination sequence number. Hence a secure routing is provided with the proposed solution. Simulation is carried out using NS2. Simulation results validate the effectiveness of our proposed schemes. The experimental results prove that the proposed solution improves the network performance. The proposed defense mechanisms can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks. As a future work, we plan to experiment the proposed scheme for securing the network with other routing protocols and also to experiment the scheme for Preventing Cooperative Attacks in Mobile Ad Hoc Networks.

*References:*


[1] S.A.Arunmozhi and Y.Venkataramani, A Flow Monitoring Scheme to Defend Reduction-of-Quality (RoQ) Attacks in Mobile Ad-hoc Networks, *Information Security Journal: A Global Perspective*, Vol.19, No.5, 2010, pp. 263- 272.

[2] Jelena Mirkovic and Peter Reiher, D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks, *IEEE Transactions On Dependable And Secure Computing*, Vol. 2, No. 3, 2005, pp. 216-232.

[3] Ping Yi, Zhoulin Dai, YiPing Zhong and Shiyong Zhang, Resisting Flooding Attacks in Ad Hoc Networks, *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)*, Vol. 2.

[4] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks, *IEEE Transactions on Consumer Electronics*, Vol. 56, No. 2, May 2010, pp. 579-582.

[5] N. Karthikeyan, V. Palanisamy and K. Duraiswamy, Optimum Density Based Model for Probabilistic Flooding Protocol in Mobile Ad Hoc Network, *European Journal of Scientific Research*, Vol.39, No.4, 2010, pp.577-588.

[6] Xuan Yu, A Defense System On Ddos Attacks In Mobile Ad Hoc Networks, *Ph.D dissertation, Auburn University, Alabama,* May 2007.

[7] Ming-Yang Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, *Computer Communications*, Vol. 34, 2011, pp. 107–117.

[8] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci and Edward Knightly, DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks, *IEEE/ACM Transactions On Networking*, Vol. 17, No. 1, February 2009, pp. 26-39.

[9] Amey Shevtekar and Nirwan Ansari, A router-based technique to mitigate reduction of quality (RoQ) attacks, *Computer Networks*, Vol. 52, 2008, pp. 957–970.

[10] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, *International Journal of Information Technology*, Vol. 11, No. 2, 2005, pp.83-94.

[11] Michele Nogueira Lima, Aldri Luiz dos Santos and Guy Pujolle, A Survey of Survivability in Mobile Ad Hoc Networks, *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 1, 2009, pp. 66-77.

[12] S.Sanyal, A.Abraham, D. Gada, R.Gogri, P.Rathod, Z.Dedhia and N.Mody, Security scheme for distributed DoS in mobile adhoc networks. *ACM, New York*, 2004.

[13] H. Deng, W. Li and D.P.Agrawal, Routing security in wireless ad hoc networks, *IEEE Communications Magazine*, Vol. 40, No. 10, 2002, pp. 70- 75.

[14] P.Ebinger and M.Parsons, Measuring the Impact of Attacks on the Performance of Mobile Ad hoc Networks, ACM PE-WASUN: *Proceedings of the 6th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Network*, 2009.

[15] Zhiqiang Gao and Zhiqiang, Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests, *IEEE Communications Letters*, Vol. 10, No. 11, 2006, pp. 793-795.

[16] Junhai Luo, Mingyu Fan and Danxia Ye, Black Hole Attack Prevention Based on Authentication Mechanism, *11th IEEE Singapore International Conference on Communication Systems*, 2008, pp.173-177.

[17] Elmar Gerhards Padilla, Nils Aschenbruck, Peter Martini, Marko Jahnke, and Jens T¨olle, Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, *Proceedings of 32nd IEEE Conference on Local Computer Networks*, 2007, pp. 1043-1052.

[18] M.Al-Shurman, S.Yoo and S.Park, Black hole Attack in Mobile Ad Hoc Networks. *ACM Southeast Regional Conference*, 2004, pp. 96-97.

[19] Jieying Zhou, Junwei Chen and Huiping Hu, SRSN: Secure Routing based on Sequence Number for MANETs, *International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp.1569-1572.

[20] Nital Mistry, Devesh C Jinwala and Mukesh Zaveri, Improving AODV Protocol against Blackhole Attacks, *Proceedings of the International Multiconference of Engineers and Computer Scientist*, Hong Kong, Vol. II, 2010.

[21] Z.Gao and N.Anzari, Differentiating malicious DDoS attack traffic from normal TCP flows by proactive tests, *IEEE Communications Letters*, Vol. 10, No. 11, 2006, pp. 793-795.

[22] X.Wu and D.K.Y Yau, Mitigating denial-of-service attacks in MANET by distributed packet filtering: A game-theoretic approach, *Proceedings of the 2nd ACM Symposium on Information, Computer and Communication Security*, 2006, pp. 365–367.

[23] P.Ebinger and M.Parsons, Measuring the impact of attacks on the performance of mobile ad hoc networks. *ACM PE-WASUN: Proceedings of the 6th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, Canary Islands, Spain, 2009.

[24] J.Haggerty, Q.Shi and M.Merabti, Statistical signatures for early detection of flooding denial-of-service attacks, *Security and Privacy in the Age or ubiquitous Computing, IFIP Advances in Information and Communication Technology*, Vol. 181, 2005, pp. 327-341.

[25] X.Luo, E.W.W.Chan and R.K.C.Chang, Detecting pulsing denial-of-service attacks with nondeterministic attack intervals, *EURASIP Journal on Advances in Signal Processing*, Vol.2009, pp.1-13.

[26] S. Buchegger and J. Boudec, Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, Canary Islands, Spain, 2002.

[27] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, *Proc. of the Sixth Annual International Conference on Mobile Computing and Networking* (MOBICOM), Boston, 2000.

**S. A. Arunmozhi** obtained her B.E. degree from Regional Engineering College, Trichy, and M. Tech. from National Institute of Technology, Trichy. She is an Associate Professor at Saranathan College of Engineering. Her research interests are in Computer Networks and Wireless Network Security.

**Dr. Y. Venkataramani** obtained his B. Tech. & M. Tech. degrees from Indian Institute of Technology, Chennai, and Ph.D. from Indian Institute of Technology, Kanpur. He has served as a faculty for 34 years at National Institute of Technology, Calicut. He is presently Dean (R & D) and P.G. Professor at Saranathan College of Engineering, Trichy. His areas of interest of include Computer Networks, Speech Processing and Image Processing.