Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs

K.Selvavinayaki
Lecturer
Dept of Comp.Science
Sree Narayana Guru College
Coimbatore

K.K.Shyam Shankar
Lecturer in MCA Dept
Sri Venkateswara College
Coimbatore

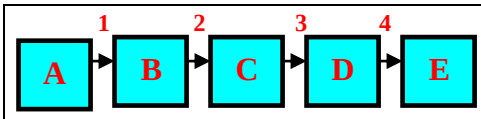
Dr.E.Karthikeyan
Asst.Professor
Dept of Comp.science
Govt.Arts College
Udumalpet-Coimbatore

ABSTRACT
The dynamic changing nature of network topology makes any node in MANET to leave and join the network at any point of time. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. The routing attack addressed in this paper is the black hole attack. The Black hole attack is that where a malicious node advertises itself as it is having the optimal route to the destination. Most of the Routing protocols do not address the issues of the routing attack. This paper describes a solution strategy which will overcome the black hole attacks in MANETs. The proposed solution is that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on DSR protocol .This method is capable of detecting and removing black hole nodes in the MANET.

Keywords
Black hole attack, DSR, Security certificate.

1. INTRODUCTION
MANET provides a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate through the fixed structures. Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.
The routing protocols for adhoc networks are Proactive routing protocol and Reactive routing protocol. The proactive routing protocols are Table driven. A routing table is maintained by each node in the network. The table contains the routing entries for all the possible nodes in the MANET. The reactive routing protocols are on demand routing protocols. The routes are propagated only on demand. Dynamic Source Routing (DSR) and AODV are on demand routing protocols. DSDV is a table driven routing protocol. These are the commonly used protocols in MANETs.[2]
DSDV maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead also grows .DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node.

1.1.Over view of DSR 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. The protocol is composed of the two mechanisms of *Route Discovery* and *Route Maintenance*, which work together to allow nodes to discover and maintain *source routes* to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely *on-demand*, allowing the routing packet overhead of DSR to scale *automatically* to only that needed to react to changes in the routes currently in use. _
Route Discovery is the mechanism by which 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 **D** and it does not already know a route to **D**. [1]
When some node **S** originates a new packet destined to some other node **D**, it places in the header of the packet a *source route* giving the sequence of hops that the packet should follow on its way to **D**. Normally, **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**. **S is** the *initiator* and **D is** the *target* of the Route Discovery.
To initiate the *Route Discovery* [1], **the source transmits** a ROUTE REQUEST (RREQ) message as a single local broadcast packet, which is received by (approximately) all nodes currently within wireless transmission range of **source**. Each RREQ message identifies the initiator and target of the Route Discovery, and also contains a *unique request id*, determined by the initiator of the REQUEST. 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. This route record is initialized to an empty list by the initiator of the Route Discovery.



1. **A----->.B (A) ID=2**
2. **B---- > C : (A,B) ID=2**
3. **C---->-D;(A,B,C) ID=2**
4. **D----> E(A,B,C,D) ID=2**

Figure.1. Route Discovery Process

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, giving a copy of the accumulated route record from the RREQ; when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. Otherwise, if this node receiving the RREQ has recently seen another RREP message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the RREQ message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet with the same request id.

Route Maintenance [1] 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*. In particular, unlike other protocols, DSR requires *no* periodic packets of *any kind* at *any level* within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to *zero*, 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 (as well as through routing information from other packets overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks.

When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. For example, in the situation illustrated in Figure 2, node **A** has originated a packet for **E** using a source route through intermediate nodes **B**, **C** and **D**. In this case, node **A** is responsible for receipt of the packet at **B**, node **B** is responsible for receipt at **C**, node **C** is responsible for receipt at **D**, and node **D** is responsible for receipt finally at the destination **E**. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use such as the link-level acknowledgement frame defined by IEEE 802.11 or by a *passive acknowledgement*. If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR-specific software acknowledgement be returned by the next hop; this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is uni-directional, this software acknowledgement may travel over a different, multi-hop path. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. For example, in Figure 2, if **C** is unable to deliver the packet to the next hop **D**, then **C** returns a ROUTE ERROR to **A**, stating that the link from **C** to **D** is currently "broken." Node **A** then removes this broken link from its cache; any retransmission of the original packet is a function for upper layer protocols such as TCP. For sending such a retransmission or other packets to this same destination **E**, If **A** has in its Route Cache another route to **E** (for example, from additional ROUTE Reply's from its earlier Route Discovery, or from having overheard sufficient routing information from other packets), it can send the packet using the new route immediately. Otherwise, it may perform a new Route Discovery for this target

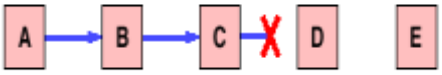


Figure2: Route Maintenance Process

The operation of Route Discovery and Route Maintenance in DSR are designed to allow uni-directional links and asymmetric routes to be easily supported. In particular ,in wireless networks, it is possible that a link between two nodes may not work equally well in both directions, due to differing antenna or propagation patterns or sources of interference. DSR allows such uni-directional links to be used when necessary, improving overall performance and network connectivity in the system.. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available. For example, some nodes in the ad hoc network may have only short-range radios, while other nodes have both short-range and long-range radios; the combination of these nodes together can be considered by DSR as a single ad hoc network.

A node forwarding or otherwise overhearing any packet may add the routing information from that packet to its own Route Cache. In particular, the source route used in a data packet, the accumulated route record in a ROUTE REQUEST, or the route being returned in a ROUTE REPLY may all be cached by any node.

1.2. Black Hole Attacks

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that a malicious node can execute is to stop forwarding the data packets. As a result, when the malicious node is selected as a route, it denies the communication to take place.

In black hole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination.

The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a

black hole as it swallows all objects and data packets . Co operative Black hole means the malicious nodes act in a group However, in reality, the packets are consumed by node

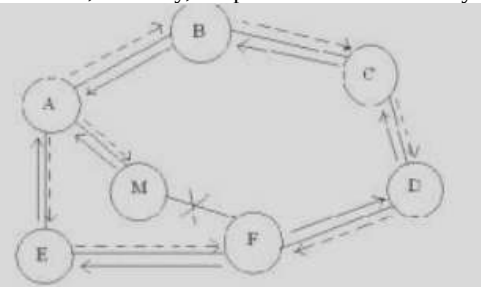


Figure 3: Black hole Attack

For example, source A wants to send packets to destination D, in Figure3, source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination. Node M claims to have the route to destination and sends reply RREP packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing cache as the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped. The malicious node forms a black hole in the network and this problem is called black hole problem.

2. RELATED WORK

Many routing protocols has been proposed for adhoc routing. The DSR protocol is a reactive protocol which is only used when new destinations are sought; during a route breaks or a route is no longer in use.

Many researchers have addressed the black hole attack problem in MANET. All the solutions proposed and implemented were based on AODV and DSDV protocol.

Marti, S., Giuli, T. J., Lai,K., & Baker, M.[5] have proposed a Watchdog and Path rater approach against black hole attack which is implemented on top of source routing protocol such as DSR (Dynamic Source Routing).

CONFIDANT (Cooperative of Nodes, Fairness In Dynamic Ad-hoc Networks) is an extended version of Watchdog and Path rater which uses a mechanism similar to Pretty Good Privacy for expressing various levels of trust, key validation and certification. It is also implemented on unicast routing protocol such as DSR.

E.A Mary Anita et al [3] proposed a solution implemented on the top of ODMRP protocol. The authors proposed a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority.

Sanjay Ramaswamy, et al [7] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

Latha Tamilselvan, Dr. V Sankaranarayanan[9] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having '0' value is considered as malicious node and is eliminated.

Hesiri Weerasinghe [4] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the S.Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP).

Most of the papers have addressed the black hole problem on the protocol such as AODV. This paper presents a solution SC-DSR scheme, which is implemented on the top of the route discovery process in DSR.

This algorithm is a modified version of the DSR to detect and prevent the black hole nodes in the MANET

3. PROPOSED SOLUTION.

Public Key Infrastructure (PKI)is one of the most effective tools for providing security for dynamic networks.. The proposed scheme uses the route discovery scheme of DSR to issue security certificates. Since there is no fixed infrastructure, nodes carry out all required tasks for security solutions including routing and authentication in a self organized manner.

3.1 Digital signature security scheme.

The digital signature is a security Certificate which is a self organized and PKI authenticated by a chain of nodes without the use of a trusted third party. Authentication is represented as a set of security certificates that form a chain. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range of each other. A certificate is a binding between a node, its public key and the security parameters Certificates are stored and distributed by nodes themselves. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice, one by the issuer and the other for whom it is issued. Periodically certificates from neighbors are requested and routing cache is updated by adding new certificates. If any of the certificates are conflicting, i.e., same public key to different nodes or same node having different public key, it is possible that a malicious node has issued a false certificate A node then labels such certificates as conflicting and tries to resolve the conflict. If certificates issued by any node are found to be wrong, then that node may be assumed to be malicious. If multiple certificate chains exist between a source and destination, the source selects a chain or a set of chains for authentication. DSR authentication uses security certificate chain.

E.A Mary Anita et al [3] proposed a solution implemented on the top of ODMRP protocol. The authors proposed a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key

without the need of any online centralized authority. The major draw back here is, it results in the increased routing overhead since it records all the certificates issued to each other neighbors and certificates received from all the neighbors. When the number of nodes in the network increases the memory consumption to design the routing table is not tolerable. We propose to modify the mentioned solution and implement on the top of the route discovery process in DSR.

The DSR protocol comes with the routing cache , which stores the route for each node in the network. This routing cache can be refreshed periodically to store the fresh routes.

SC-DSR (Security Certified DSR) is a extension of DSR where the route discovery phase is extended and messages are signed to guarantee their authentication. The extended route discovery process of DSR consists of the original route discovery process followed by an authentication phase.

Once the route is established between the source and the destination, the nodes forming the route enter into an authentication phase. The source node requests the identity of the next hop node and generates a public key based on its identity. The security parameters of the next hop node are then requested and security certificates are issued if the issuer is convinced about the security parameters.

The time taken to process the RREQ packet and the location of the node are ideal parameters to determine the security level of the node with respect to black hole attack.

The Malicious node which receives the RREQ replies by sending the RREP immediately without a time delay. In this case the source node sets a minimum time delay to receive the RREP. If it receives the RREP too earlier, then the source suspects the RREP initiator to be black hole node and initiates the black hole node detection and removal process.

All security certificates issued are stored in the repositories of the issuer and the certificate subject. Exchange of certificates between neighboring nodes takes place periodically. By this certificate exchange mechanism, nodes accumulate certificates in their repositories at a low communication cost because the exchanges are performed locally in one hop.

For example if node B is within the radio range of node A, node A issues a certificate to B.

$$SC(A \rightarrow B) = \{ ID\_B, key\ B, ET, Sv, \} KeyA$$

The certificate contains the identity of node B, the public key of B, the time of issue of the certificate, the time of its expiry and the security level of the node, signed by the public key of A.ID may be the IP Address of the B node.

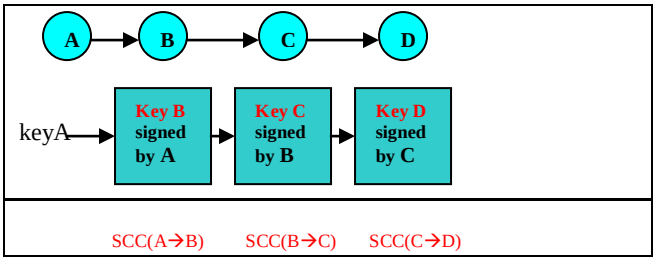


Figure 4.certificate Chain model

Key B is the Public key generated by applying one way hash function to IP address of the node. Initially the Sv value is set to 1 if an issuer node is convinced of the security parameters of the subject node. If security is found to be compromised, the Sv is reduced to zero. A node bearing a certificate with Sv=0 is set aside as malicious node.

Every security certificate becomes invalid when the ET value expires. However if the certificate is still required to be used, the issuer has to update the certificate if it is still convinced about the security level of the subject node. On the other hand, if the issuing node feels that the subject node is compromised, it will not provide the certificate update. If the Sv value of the Certificate is not to the satisfactory level then certificate issued to the node will be revoked

3.2. Authentication

When a source node S wants to find a route to a destination node D, it broadcasts a RREQ packet to the neighboring nodes. The destination node or any other node that has a valid route to the destination now replies to the RREQ. The RREP packets in SCDSR are similar to that DSR. Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination.

To overcome this black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination. The destination node sends authenticated messages appended with certificates taken from the corresponding node's repository.

The authenticated RREP packet from the destination would be of the form

[Source id, next hop id, final destination id, SCC]

For Example in Figure 5

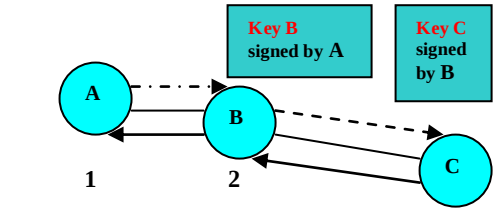


Figure 5.Certiifed Route from Source to Destination

The RREP cert packet from C would be

[C, A, SCC (B→ C)]

When this packet reaches node B, It checks its routing cache to see if SCC (B-→C) is there. It checks where C is a malicious node are not by checking the SCC(security certificate chain) issued list If C is a promiscuous node then it forward the RREP packet to A by append the SCC(A→B)

The Forwarded RREP will be in the Form of

{C,A, A, SCC (A→B), SCC (B→ C)]

All intermediate nodes perform the same procedure until the final destination A is reached. When node A receives the packet, it checks the whole certificate chain. If there is no problem with the certificate chain, node A trusts the route and starts sending data packets through this route and in case of a legitimate node turning malicious over a period of time, the node's behavior would be recorded and once recorded the certificate would not be renewed after its expiry time, thus isolating the node from further participation in the network activities.

Since the security levels of participating nodes are updated based on their faithful participation in the network, any malicious nodes between the source and destination can be very well isolated from the network as these nodes would not be able to produce the certificates to be appended with the RREP message.

3.3.Algorithm

SN – Source , IN- Intermediate node, DN-Destination ,NHN-Next Hop Node

Step 1:

SN broadcasts RREQ
IF (IN is NOT DN) THEN
Rebroadcast RREQ
ELSE DN return RREP
{ DN unicasts JREP
All INs forward the RREP
RREP reaches SN}
Route is established between SN and DN

Step 2:

Set Delay time. Sv=0.
If RREP Time is Earlier than the Delay time
Do not Issue Security Certificate. Check the route cache for alternate route.
Else
Nodes forming the route certify each other:
Request id and security parameters of NHN
Generate public key of NHN based on id
Issue Certificates encrypted with public key
Store certificates in route cache
Exchange Certificates with neighbor nodes

Step 3

DN sends certified RREP appended with security certificate from NHN
All INs append their certificates and forward the certified RREP
RREP reaches SN
SN verifies certificate chain and Routes data packets through the secure path.

The main Advantage of modifying the DSR protocol with is algorithm to prevent black hole attacks may show a improved performance. The memory overhead can be reduced, since the certificate can be added to the routing information already available in the Routing cache of the DSR. Since routing cache can be refreshed frequently the possibilities of increased memory overhead may be minimized.

4. CONCLUSION

In this paper we have mentioned the routing security issues of MANETs and the cooperative black hole attack in MANET. We have proposed a feasible solution for the black hole attacks that can be implemented on the DSR protocol. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio, mean delay time, packet overhead, memory usage and scope of the black hole nodes.

REFERENCES

[1].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.

[2] D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4,4th Quarter 2005.

[3] E. A. Mary Anita and V. Vasudevan, Black Hole attack Prevention in multicast routing Protocols For MANETs Using Certificate Chaining, IJCA, Vol.1, No.12, pp. 22–29,2010

[4]Hesiri Weerasinghe and Huirong Fu, Member of *IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation ImplementationAndEvaluation,IJSEA,Vol2,No.3,July 2008.*

[5] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000),Mitigating routing misbehavior in mobile ad-hoc networks, Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-58113-197-6, pp. 255-265.

[6] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black andGray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the

2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[7].Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.

[8]Sukla Banerjee ,Dectection /Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-hoc Networks. Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[9] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET",JournalOfNetworks ,Vol.3,No.5,May2008.

[10] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540-7993/04/$20.00 © 2004 IEEE, May/June 2004.