Abstract
Background/Objectives: A Mobile Ad-Hoc Network is formed with an assembly of mobile nodes. Efficient data transmission with security is the important requirement. Security vulnerabilities like attacks are high in MANET. One of the vital attacks is Black hole attack. Methods/Statistical Analysis: The objective of this article is to transmit data in efficient way and also in secured manner. This paper suggests a Secured Direction Oriented Forwarding through Minimum amount of Edge Nodes (SDOF-MEN) protocol for MANET. By reducing the amount of transmissions the efficiency can be improved. Secured transmission is achieved by identifying and removing Hateful nodes from the network. Findings: The SDOF-MEN Protocol is a method which selects least amount of edge nodes to communicate the data. It picks one particular verge node as following hop, and transmits data to the selected following node only. Hence the routing overhead is completely reduced. Thereby it reduces the amount of path-finding messages. With respect to the location, the information is straightly conveyed through midway nodes, hence the efficiency of the whole network is increased. Some nodes are Hateful nodes which are dropping data packets. It identifies both internal and external black hole nodes and removes from the data transmission process. Applications/Improvements: In this paper the algorithm is simulated using ns-2 simulator and analyzed by measuring the performance parameter Packet Delivery Ratio. The Packet Delivery Ratio can be enriched by removing Hateful node.

Keywords: Base Station, Black Hole Attack, Mobile Ad-Hoc Network, Reduced Path-finding Overhead, Routing Through Edge Node, Secured Transmission

1. Introduction
To make effective communication in the MANET the nodes of the network must cooperate in the communication process. In MANET the communication takes place in a multi hop mode. In multi-hop MANET all the nodes are having limited energy source and so planning of the energy-efficient routing protocol is critical. The secured data routing is also difficult because some nodes are Hateful. In recent years many security concerns have been identified and considered. For example, snooping attacks, wormhole attacks, black hole attacks, packet duplication, repudiation of service (RoS) attacks, distributed RoS (DRoS) attacks, especially, one of the spread security threats is the misbehavior routing problem such as black hole attacks.

1.1 Proactive (Table-driven) Protocols
The proactive direction-finding protocol uses direction-finding tables. They gather facts sporadically from neighbors and saves in the table. The tables are of different types. For each and every change in the network updating the routing table is must. For each neighbor one entry is there. Some proactive routing protocols are analyzed in and. The proactive routing protocol is easy for small dimension network and difficult for large network due to table maintenance. The power consumption, Routing
overhead and Bandwidth are high for large network. Hence it is not fit for large network.

1.2 Reactive (On-Demand) Protocols
The reactive protocols are not using direction-finding tables. When one node wants to communicate to a different node, it starts path identification process. When discovers the path the node will send information through that path. Hence it reduces the routing overhead likened with Proactive direction-finding protocol. But it raises the delay. During route identification process, the source node broadcasts the request packet to all existing neighbors.

1.3 Hybrid Direction-finding Protocols
Hybrid direction-finding protocol incorporates the benefits of both proactive and reactive protocols. Every one describes two regions: the inner region and the outer region. Thus, the hybrid protocols follow the routing procedure of the proactive protocols in the inner region and procedure of the reactive protocols in the outer region. The Zone Routing Protocol (ZRP) is a sample of Hybrid direction-finding protocols.

1.4 Flooding
It is the simple path detection algorithm. Maximum of the direction-finding protocols are using flooding to catch the path in the middle of source and destination. (DSR, AODV). Flooding includes all the nodes in the communication process. It decreases the energy of completely the nodes and thereby the network lifetime. The possibility of black hole attack is high. Identification of the black hole node is difficult.

1.5 Location-Aided Routing (LAR) protocol
LAR be influenced by the locality info of the nodes which is found with a scattered locality service. LAR protocol habits locality information to lessen the examine space for a wanted route. The search area is reduced as a small rectangle in which both the source and receiver are there. It includes the nodes which are in the interior of the rectangle. The nodes outside of the rectangle are not involved so that their energy is saved. Hence the network lifespan is enlarged. But it implicates one collection of nodes and the energy of those nodes would be reduced.

The nodes in the region border which gets the IERP demand packet will add 1 with the BH value. At that time the node verifies the terminus in its direction-finding table, if the terminus address doesn’t available in its direction-finding table, at that time it would go on with the boundary selection formula. While the node discovers the terminus in its direction-finding zone or itself a terminus, at that time the node will reply with IERP Reply packet. Here all the zone border nodes are involved in data routing process. Thereby the efficiency of the network is reduced.

1.6 Black Hole Attacks Detection by Invalid IP Addresses
This method supports to discover the Hateful nodes consuming legal and illegal addresses, without activating untrue finding through the network. But sometimes the node with valid IP addresses can be a Hateful one. It can identify the Hateful node but cannot prevent data.

Figure 1. The network with Base Station contains eight regions.

1.7 Kuder-Richardson Reputation Co-efficient based Cooperation Enforcement Mechanism (KRRCM)
It is for mitigating Root node attack based on Kuder-Richardson Reputation Co-efficient (KRRC) that calculates the reputation level of mobile node. This Kuder-Richardson Reputation Co-efficient is calculated based on second hard reputation. The coefficient value obtained through KRRCM approach reflects an individ-
ual root node's behavior in relation to cooperation, so that the particular node can be selected as core point for group communication\textsuperscript{13}.

1.8 Ticket based Routing Algorithm

The ticket centered direction-finding uses one searching packet to discover the state of the traversed path. The state information is the path, the end to end delay and the cost. Two color tickets are available. One is green ticket which indicates the optimized end to end cost. Another is yellow ticket which indicates the feasible path and less end to end delay\textsuperscript{14}.

2. Secured Direction Oriented Forwarding through Minimum Amount of Edge Nodes (SDOF-MEN) Protocol for MANET

In this protocol the amounts of route detection messages are reduced. Only one node is selected as following hop and its address is added. The selected node receives and transmits the data. The next hop is selected based on the location of the receiver. The second next hop is also selected following the same procedure. The selecting node verifies that the receiver is its neighbor. If it is its neighbor, it directly transmits the data. If it is not its neighbor, one of its verge nodes will be selected as following hop\textsuperscript{13}.

The Direction Oriented Forwarding through Minimum amount of Edge Nodes (DOF-MEN) protocol\textsuperscript{3,15} is an alteration to the ad hoc direction-finding protocols EELAR and ZRP. This protocol lessens the amount of way finding messages. It efforts to choose single node as following hop. Later the particular node alone will accept and then frontwards the data. It recognizes the locality of the receiver node. If the receiver node is not in the region of the transmitter node, it picks lone one verge node for dispatching. It does not direct to all the verge nodes.

The BS maintains one special table for black hole nodes. In this table the information of the black hole nodes is available. The BS periodically broadcasts the Black Hole Table (BHT). The Transmitter Node (TN) first checks the BHT to identify whether the Receiver Node (RN) is a black hole node or not.

2.2 Data Transmission

If Transmitter Node (TN) wishes to direct documents to some Receiver Node (RN), Initially it scans its tables. If the record exists, it could openly direct the information to the Receiver Node (RN). It appends the label of the node in the receiver node address field. If it does not exist, it will direct demand packet to the BS to acquire the position of the node. The BS guides the position ID of the Receiver Node. After getting the ID of the RN, the TN begins the transmission process\textsuperscript{3}. The transmitter node chooses the verge node in matching way of receiver node as Next Hop (NH). The Transmitter Node (TN) then checks the BHT to identify whether the Next Hop (NH) is a black hole node or not.

Figure 2 displays the procedure of next hop selection in SDOF-MEN protocol. The transmitter node chooses one of its verge nodes as NH. The nominated node will be performing as new transmitter and picks one of its verge nodes as NH. In that way the data is accelerated through verge nodes to receiver.

2.3 Security Attacks

Security is an important think in all communication processes. In MANET the transmission medium is an open medium, Topology is dynamic, and Nodes can join and leave from any group easily. Hence MANET suffers easily suffers from security attacks\textsuperscript{16}. 

Vol 9 (S1) | December 2016 | www.indjst.org

R. Suganthi and S. Sankara Gomathi
Secured Direction Oriented Forwarding through Minimum Amount of Edge Nodes (SDOF-MEN) Protocol for MANETS

// Transmitter Node ID (θ_T, r_T),
// Receiver Node ID (θ_R, r_R)
// Transmitter node likens the IDs to find the next hop

if θ_T = θ_R//(TN and RN are in similar region)
// Then likens the radius value.

if r_T > r_R then
TN selects the Edge Node(EN) with ID (θ_T, r_T - 2)
else
TN selects the EN with ID (θ_T, r_T + 2)
end
TN communicates through the selected Verge node

else If θ_T ≠ θ_R then

if θ_T + θ_R = 0 or 180 then
Pick the neighbor within the similar region.

TN picks the EN of ID (θ_T, r_T - 2)
else Calculate D1=|θ_R - θ_1| and D2=|θ_R - θ_2|then
Pick the node in direction with minimum D as next hop
end

end

Figure 2. The scheme of Next Hop selection in SDOF-MEN protocol.

One common attacks are a Black hole attack. Some nodes are Hateful nodes. Those nodes are called as black hole nodes. One Hateful node exploits the direction-finding protocol and drops the direction-finding packets but does not accelerative packets to its neighbors. A solo black hole attack is simply occurred in the mobile ad hoc networks. A Hateful node probably droplets or consumes the packets.

In MANET, Passive and active attacks are available. The nodes are forwarding the data on their own responsibilities. Here no administrative control. So some attackers are attacking the communication process. Mobile nodes existing inside the assortment of wireless link can eavesdrop and even take part in the network.

External attackers are available at outside of the network. Those attackers are accessing the network, sending bogus packets, denial of service. We can prevent these attacks by proper implementation. Some nodes are internal nodes which are having access to the network. They are dropping packets, sending bogus packet.

2.4 External Black hole attack

External attackers really halt outer of the network and they don’t have rights to access the network. They are trying to create attacks in the network. They don’t forward packets. They are dropping or using the packets. It reduces the network efficiency. Hateful node observes the alive way and notes the receiver address. Hateful node changes the route answer packet (RREP) thus creating one loop connection between transmitter and receiver nodes. Thereby it introduces congestion in the network.

Hateful node directs a Route Reply Packet (RREP) containing the receiver address field bluffed to an unfamiliar receiver address. Hop sum value is set to lowermost values and the sequence number is set to the maximum value. Hateful node involves itself in the transmission path by sending reply to the nearest neighbor of the transmitter node. The transmitter node believes the nearest neighbor, so it transmits data through the node. The Hateful node will fall now all the data to which it has its place in the route.

2.5 Solution to External black hole attack in DOF-MEN protocol

For each and every node one Private Key (PrK) and Public Key (PuK) is assigned. Each node produces its individual public key and private key. Each node stores it public key in the position table of the Base Station. The BS stores the public key of all the nodes available in the network.

The transmitter encrypts the data packet by using the public key of the receiver. The actual receiver decrypts the data packet by using its private key.

2.5.1 First Level Encryption

The Transmitter Node gets the public key of the Receiver Node. It encrypts the data by using the public key of the Receiver Node.

2.5.2 Second Level encryption

After selecting the NH, the node does the second level encryption by using the public of the selected NH. During the second level encryption the data packet along with the Transmitter node address and Receiver node address
is encrypted. The actual selected node only can decrypt the data. After decryption only it can identify the address of the receiver node. The external attacker node cannot decrypt the data. Figure 3 shows that the Transmitter Node (TN) encrypts the data first with the public key of the Receiver Node, and then encrypts it with the public key of the selected First Hop Node (FHN). FHN decrypts the received data by using its own Private Key and then encrypts the data with the Public Key of the Second Hop Node (SHN). All the nodes are following the same procedure. Finally, the Receiver Node receives the data and decrypts it with its Private Key and after identifying its own address in the destination address field it saves the data.

Figure 3. Data transmission by using SDOF-MEN protocol.

Figure 4 shows the data encryption method followed in SDOF-MEN protocol. In first level encryption the actual data is encrypted using the public key of the receiver node. In second level encryption the encrypted data and the address of both transmitter node and receiver node are encrypted by the public key of the selected next hop node. Hence the particular node only can decrypt and identify the addresses. The attacker or any other node cannot decrypt the data.

This Internal black hole attack has an interior Hateful node which fits in the middle of the paths of given transmitter and receiver. The Hateful node is acting as a data transmitter. The Hateful node transmits its own wrong data. It does not forward the actual data. It is difficult to find the internal Hateful node because the node itself is present in the transmission path.

Figure 4. Data Encryption procedure in SDOF-MEN protocol.

2.6 Internal Black Hole Attack

The Hateful node is an interior node which lies in the transmission path in the middle of the transmitter and the receiver. It can drop packets or modify the packet. In DOF-MEN, if the selected NH node is a Hateful one the data packets are dropped. The Transmitter Node first checks the status of the Next Hop as either it is a black hole node or not. If it is an external Hateful node it can be identified and removed by using the previous rule. If it is an internal registered node and if it is acting as good till that time and now it behaves in Hateful manner, the transmitter node will send data to that node. It will drop the packets. It cannot read data because of the encryption. But it can drop the packets or forward the packet in wrong direction by changing the receiver node address.

2.7 Solution to Internal Black Hole Attack in DOF-MEN Protocol

Figure 5 shows the procedure to identify the Internal Black node. To identify the Internal black node, the Base Station sends one beacon signal to the receiving node that
the particular transmitter node got its ID to transmit the data. From the beacon signal the receiver node calculates the time required to get data from the actual transmitter node. If it gets data within that interval it will accept. If it does not receive any data within the time interval it will send one special beacon signal to the Base Station. The Base station send one beacon signal to the transmitter node about this problem. The transmitter node now identifies the black hole node in its transmission path.

// Transmitter Node ID ($\theta_T, r_T$),
// Receiver Node ID ($\theta_R, r_R$)
// Receiver node relates the IDs

If $\theta_T = \theta_R$ // (both are in similar region)
RN calculates the distance $dist = (r_T - r_R)$
And calculates the time to receive the data.
Else Calculate $D_1 = |\theta_R - \theta_1|$ and $D_2 = |\theta_R - \theta_2|$ then
Select the min $D$, Calculate $f= D/45$
Calculate Radial Distance $RD = (2\pi r_T)^*(f/8)$
Calculate the distance $dist = RD + (r_T - r_R)$
And calculates the time to receive the data.
End
If RN does not receive data within the time
RN send beacon signal to Base Station (BS)
End

Figure 5. The scheme of Next Hop selection in SDOF-MEN protocol.

3. Simulation and results

NS2 is used to simulate and analyze the projected protocol. It is a Discrete Incident Simulator used to do examination in networking. The simulation produces output in the form of one trace file which is used to estimate the act metrics. The AWK software design language is used to examine the trace file. It is used to excerpt the desired data from the trace file and also used to calculate the performance parameters. Here 10 nodes are used for examination. The simulation is for 10 sec.

3.1 Packet Delivery Ratio

The proportion in the middle of the amount of data packets created by the transmitter nodes, and the amount of data packets received by the receiver nodes. The proposed protocol increases the Packet Delivery Ratio. In the trace file the forth Column registers the module in which the action is performed. The fifth Column registers the sequence number of the packet. The sequence number is used to estimate the total amount of packets created by the Transmitter Node. Packet Delivery Ratio is calculated by using total amount of packets created and the overall amount of packets supplied.

Figure 6 shows that the Packet delivery ratio is high in Secured DOF-MEN protocol than the existing protocols.

4. Conclusion

In this paper we analyzed the act of the DOF-MEN protocol. It reduces the routing overhead by reducing the searching area. It selected only one node as its next hop. In this paper we added the solutions of the black hole attack with the DOF-MEN protocol. The secured DOF-MEN protocol identifies and removes the Hateful nodes from the network. It transmits data securely. Hence it further advances the efficiency of the network.

5. References

1. Tseng F-H, Chou L-D, Chao H-C. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences. 2011; 1:4.
2. Umang S, Reddy BVR, Hoda MN. Enhanced intrusion detection system for hateful node detection in ad hoc routing protocols using minimal energy consumption. IET Communications. 2010; 4(17):2084–94.
3. Suganthi, R, Gomathi SS. Direction Oriented Forwarding with Power Adaption (DOFPA) protocol for MANETs. 2014 International Conference on Communication and Signal Processing; 2014.
4. Taneja S, Kush A. A survey of routing protocols in mobile ad hoc networks. International Journal of Innovation, Management and Technology. 2010; 1(3):279–85.
5. Rao M, Singh N. Performance evaluation of AODV nth BR routing protocol under varying node density and node mobility for MANETs. Indian Journal of Science and Technology. 2015; 8(17).
6. Rajamanickam S, Gomathi SS. Efficiency improved direction oriented forwarding protocol with the utilization of the node mobility for MANET. International Review on Computers and Software (IRECOS); 2015.
7. Kurosawa S, Nakayama H, Kato N, Jamalipour A, Nemoto A. Detecting black hole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security. 2007; 5(3):338–46.
8. Deb D, Roy SB, Chaki N. Lacber: A new location aided routing protocol for GPS scarce MANET. International Journal of Wireless and Mobile Networks. 2009; 1(1):22–35.
9. Mikki MA. Energy efficient location aided routing protocol for wireless MANETs. International Journal of Computer Science and Information Security. 2009; 4(1–2):9.
10. Haas ZJ, Pearlman MR, Samar P. The Zone Routing Protocol (ZRP) for ad hoc networks. IETF Internet Draft; 2002.
11. SreeRangaRaju MN, Mungara J. Optimized ZRP for MANETs and its Applications. International Journal of Wireless and Mobile Networks. 2011; 3(3):84–94.
12. Amiri R, Rafsanjani MK, Khosravi E. Black hole attacks detection by invalid ip addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014; 7(4):401–8.
13. Parthiban S, Rodrigues P, Kuder. Richardson reputation coefficient based reputation mechanism for isolating root node attack in MANETs. Indian Journal of Science and Technology. 2015; 8(15).
14. Hussain MA. Deployment of mobile ad-hoc network ticket based QoS routing protocol for healthcare. Indian Journal of Science and Technology. 2015; 8(15).
15. Suganthi R, Gomathi SS. Direction oriented forwarding through minimum number of edge nodes (DOF-MEN) protocol for MANETs. IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013); 2013. p. 437–42.
16. Vishnu K, Paul AJ. Detection and removal of cooperative black/gray hole attack in mobile ADHOC networks. International Journal of Computer Applications. 2010; 1(22):38–42.
17. Saini A, Kumar H. Effect of black hole attack on AODV routing protocol in MANET. International Journal of Computer Science and Technology. 2010; 1(2):57–60.
18. Himral I, Vig V, Chand N. Preventing AODV routing protocol from black hole attack. International Journal of Engineering Science and Technology. 2011; 3(5):3927–32.