MANET Routing Protocols and Wormhole Attack against AODV

Rutvij H. Jhaveri[1]
Department of Computer Engineering and
Information Technology
S.V.M. Institute of Technology
Bharuch, India

Ashish D. Patel[2]
Department of Computer Engineering and
Information Technology
S.V.M. Institute of Technology
Bharuch, India

Jatin D. Parmar[3]
Department of Computer Engineering and
Information Technology
S.V.M. Institute of Technology
Bharuch, India

Bhavin I. Shah[4]
Department of Computer Engineering and
Information Technology
S.V.M. Institute of Technology
Bharuch, India

Summary:
In this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc Network has been growing since last few years. In this paper we have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a big issue in MANETs as they are infrastructure-less and autonomous. Main objective of writing this paper is to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. This article would be a great help for the people conducting research on real world problems in MANET security.

Keywords:
Mobile Ad-hoc Network, Routing Protocols, Wormhole attack, Securing AODV, Countermeasures

1. Introduction

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration (Figure-1). Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

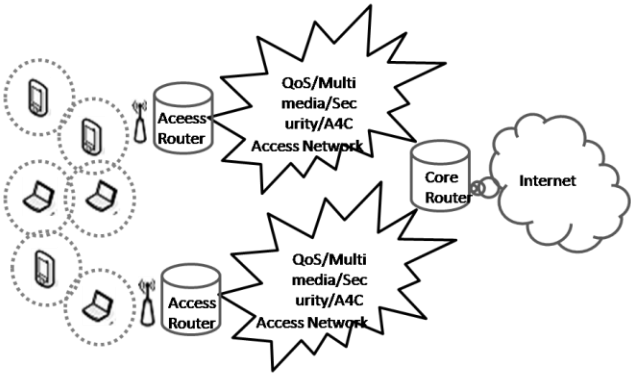

Figure-1 Mobile Ad-hoc Network [7]

There are three types of routing protocols: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency. In this paper, Sections II, III, IV and V looks at working of routing protocols like Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm (TORA) and Ad-hoc On Demand Distance Vector (AODV); Section VI thoroughly explains the exact operation of AODV. Section VII discusses some common

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

attacks against AODV in MANET; Section VIII explains the complete operation of wormhole attack against AODV; Section IX suggests some solutions to make AODV secure as well as some possible countermeasures against the wormhole attack; Section X concludes the paper.

2. Destination-Sequenced Distance Vector

Destination-Sequenced Distance Vector (DSDV) is a traditional table-driven protocol for MANET. To solve the routing loop problem, it was invented by C. Perkins and P. Bhagwat in 1994. Routes are established based on constant control traffic and they are available all the time. Each node maintains one or more tables that contain route information to other nodes in the network. Nodes continuously update the tables to provide fresh view of whole network. Updates are so frequent that the advertisement must be made regularly enough to make sure that every node can almost always find every other node in the network. The data that is broadcast by the mobile node contains its new sequence number, destination address, number of hops needed to reach destination and sequence number of the information received for the destination.

The fundamental issue with DSDV is creation and maintenance of the tables. These tables need to be frequently updated by transmission of packets, even in traffic condition. Moreover, until updates about changes in topology are not sent across the network, DSDV does not function. In a large network with high density, mobile nodes often create broken links. Maintenance and updation of tables as well as advertising the updations would be significantly complex in this kind of network. DSDV is effective for ad-hoc network with small number of mobile hosts with limited changes in network topology. Improved forms of DSDV have been suggested, but commercial implementation of the traditional DSDV has not been done.

3. Dynamic Source Routing

Dynamic Source Routing (DSR) is a reactive kind of protocol which reacts on-demand. The main feature of DSR is source routing in which the source always knows the complete route from source to destination. It frequently uses source routing and route caching. Route Discovery and Route Maintenance are two main methods used in DSR. It is uncomplicated and efficient protocol. It does not depend on timer-based activities. It allows multiple routes to destination node and routing is loop-free here. Any broken link is notified to the source node with an error message. It works well in large networks where routes change quickly and mobility of routes is higher.

In DSR, intermediate nodes do not need to preserve the routing information. Instead the packets themselves contain every routing decision. DSR uses a route discovery process to find a route when a node in the network tries to send a data packet to a destination for which the route is unknown. A route is found by flooding the network with route requests. When a node receives this request, it broadcasts it again until it itself is the destination or it has the route to the destination. This node then replies to the request to the original source. The request and response packets are source routed. Request packet creates the path of traversal. Response packet creates the reverse path to the source by traversing backwards.

4. Temporally-Ordered Routing Algorithm

Temporally-Ordered Routing Algorithm (TORA) is made to find routes on demand. It tries to achieve high scalability. It creates and maintains directed acyclic graph rooted at the destination node. TORA can establish routes rapidly and can provide multiple routes for a single destination. It doesn’t give Shortest-Path Algorithm too much of importance. Instead it uses longer paths to avoid finding of new routes. TORA minimizes communication over as it reacts only when needed and doesn’t react to every topological change as well as it localizes scope of failure reactions.

There are three main phases of the algorithm: Route Creation, Route Maintenance and Route Erasure. In the Route Creation phase, the query packet is flooded all over the network and if routes exist, an update packet is sent back. In the Route Maintenance phase update packets re-orient the route composition. The route erasure phase involves flooding of a broadcast clear packet all over the network to erase invalid routes. To simulate the protocol, size of network, rate of topological change and network connectivity should be kept in mind.

5. Ad-Hoc On Demand Distance Vector

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. It is a modification of DSDV. The demand on available bandwidth is significantly less than other proactive protocols as AODV doesn’t require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path.

6. Exploring AODV

Route discovery process is started by a source node that wants to communicate with a destination node for which there is no routing information in its routing table. Each node broadcasts a HELLO message after a specific interval to keep track of its neighbors. Thus a node keeps track of only its next hop for a route instead of entire route. When a node wants to communicate with a node that is not its neighbor it broadcasts a route request packet called RREQ which contains RREQ ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Destination Sequence Number is the latest sequence number received in the past by the source for any route towards the destination. Source Sequence Number is the latest sequence number to be used in the route entry pointing towards the source of RREQ. Every route table entry for every node must include the latest sequence number for the nodes in the network. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop Count represents the distance in hops from the source to destination [23][24][25].

When a node receives an RREQ, it checks that whether it has already received an RREQ with the same Source IP Address and RREQ ID within PATH_DISCOVERY_TIME. If yes, it discards the newly arrived RREQ. If not, it increments the hop count value in RREQ by one. The route table entry for the destination will be updated with the new sequence number if:

1. Destination Sequence Number received from RREQ is greater than the existing value in the route table entry.
2. The Sequence numbers are equal, but the incremented hop count is smaller than existing hop count.
3. The Sequence number is unknown.

Soon after this updation valid sequence number field in the route table entry is set to true. The node searches for a reverse route towards the Source IP Address. If need be, route is created or updated using the Source Sequence Number. When the reverse route is created or updated following events are carried out:

1. If Source Sequence Number received from RREQ is greater than the existing value in the route table entry, it is updated.
2. The valid sequence number field is made true.
3. The next hop in the routing table becomes the node from which RREQ was received.
4. The value of hop count is copied from RREQ packet.
5.

After updating the information the intermediate node forwards the RREQ packet until a node is found that is the destination itself or it has an active route to the destination with Destination Sequence Number greater than or equal to that of RREQ. This node replies back to the source node with a route reply packet RREP and discards the RREQ. If the node generating RREP is an intermediate node, it copies the known sequence into the Destination Sequence Number field in the RREP packet. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Lifetime represents the time in which nodes receiving RREP consider the route to be valid. When a node receives an RREP packet, it finds a route to the previous hop and increments the hop count value in the RREP by one [25]. The existing route table entry of the Destination Sequence Number is updated if:

1. The Destination Sequence Number in the RREP is greater than existing value and the value is valid.
2. The Sequence Numbers are same, but the incremented hop count is smaller than that of existing value.
3. The sequence number is marked as invalid in the routing table.
4. The sequence numbers are same, but the route is marked as inactive.

Thus, an intermediate node or a source node updates its corresponding route table entry. When the RREP reaches to the source node, it can now send the data packets through the route that is set up [23][24][25].

A node generates router error packet RRER in the following situations:

1. While transmitting the data, if it notices a link break for the next hop (neighbor) of an active route in its routing table. Here the node first makes the list of unreachable destinations along with unreachable neighbors in the routing table.
2. If it receives a data packet that is to be sent to a destination node for which it does not have an active route.
3. If it gets an RERR from a neighbor for one or more active routes.

RERR packet allows AODV to adjust routes when a node moves around in a MANET. The RRER indicates those destinations that are unreachable; each node keeps a 'precursor list' containing the IP address for each of its neighbors that are likely to use it as a next hop towards destination. The information in the precursor list is acquired during the generation of a RREP packet [23][24][25].

6.1 Looking at working of AODV

We take an example of five mobile nodes as shown in Figure-2. The circles indicate the range of communication for the nodes. As each node has a limited communication range, it can communicate with its neighbor nodes only. At an instant, Node 4 wants to communicate with Node 3, but it is uncertain of the route. Node 4 broadcasts RREQ that is received by its neighbors Node 1 and Node 5. Node 5 doesn't have any route to Node 3 and therefore it rebroadcasts RREQ that is received back by Node 4. Node 4 drops it. On the other side, if Node 1 has a greater sequence number than RREQ, it discards RREQ and replies with RREP. If not, it updates the sequence number in its routing table and forwards RREQ to Node 2. As Node 2 has a route to Node 3, it replies to Node 1 by sending an RREP. Node 1 sends RREP to Node 4 and route Node 4-Node 1-Node 2-Node 3 is confirmed to send data packets. Node 4 can now send data packets to Node 3 through the specified route. Imagine a Node 6 in the communication range of Node 1 and Node 2. As shown in Figure-3, Node 1 moves out of network. Suppose Node 6 detects it first by not getting any HELLO message from Node 1and marks the respective route table entry for route as invalid. It sends out an RERR with the invalid route which is received by Node 2. This is how Node 2 comes to know from Node 6 that Node 1 is no longer its neighbor.

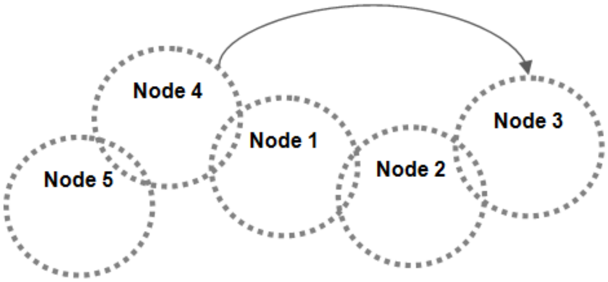

Figure-2 Communication between nodes in a Mobile Ad-hoc Network

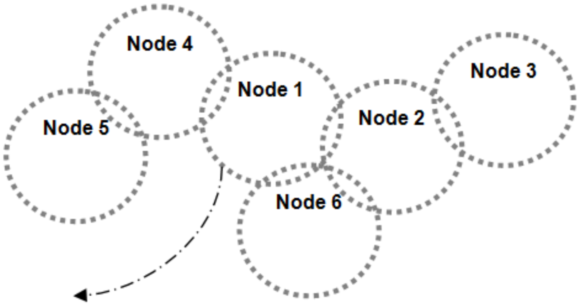

Figure-3 Node 1 moves out of communication range

7. Security Attacks Against AODV

As MANETs are unwired network with dynamic topology associated with them, they are very vulnerable to MANET attacks. In protocol stack, Physical layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Transport layer has issues with end to end data security with encryption methods and Authentication. Application layer has security concerns with prevention, worms, malicious codes, application abuses as well as virus detection.

There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET.

7.1 Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack may be launched by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

7.2 Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause lots of attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

8 7.3 Attacks using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks are described here:

1) *Blackhole attacks*: A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process. Cooperative black hole attack is caused by many neighbor black holes cooperating each other. Black hole attack may be internal or external.

2) *Grayhole attacks*: A gray hole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes. In other type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. Sometimes, a node may combine the behavior of attacks discussed above. Due to this uncertainty in behavior of gray hole, this type of attacks are more difficult compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV.

3) *Wormhole attacks:* In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called ‘wormhole link’. They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network.

8. Operation of Wormhole attack in AODV

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

Wormhole attack [20] commonly involves two remote malicious nodes shown as X and Y in Figure-4. X and Y both are connected via a wormhole link and they target to attack the source node S. During path discovery process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, receive RREQ and forward RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

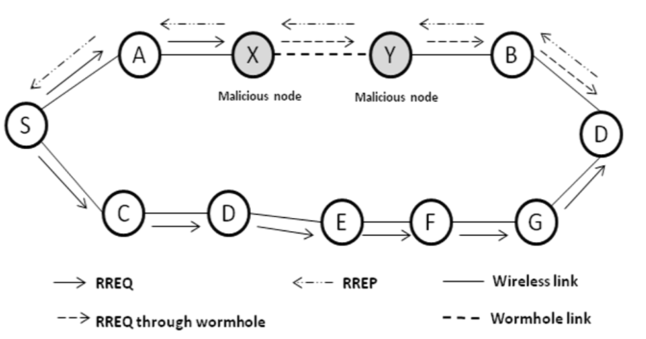

Figure-4 Wormhole attack on AODV in MANET [20]

9. Securing AODV

To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [26].

As MANETs use an open medium, all nodes can access data within the communication range. Therefore, **confidentiality** should be obtained by preventing the unauthorized nodes to access data. **Authentication** should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes. **Integrity** helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called **non repudiation** [18] [26].

To defend against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful. Encryption and authentication are based on asymmetric and symmetric cryptography [26]. To achieve data integrity and authentication, hash functions and digital signatures are really useful.

Secure Ad-hoc On Demand Distance Vector (SAODV) is an extension of AODV in which digital signature and has chains mechanisms are used. Every node uses digital signature for authentication and integrity in routing messages like RREQ, RREP and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop-count mechanism. Thus, SAODV addresses security of routing messages only; security of data exchange still remains unaddressed. Moreover, due to digital signatures, messages get bigger. Also, generating and verifying signatures add to the overhead, especially when double signatures mechanism is used.

9.1 Countermeasures against Wormhole attack

Lots of researchers have worked on techniques of detection and prevention of wormhole attack. We will discuss some of them briefly.

For detection and prevention of wormhole attacks, 'Packet Leash' mechanism is suggested in which all nodes in the MANET can obtain authenticated symmetric key of every other node. The receiver can authenticate information like time and location from the received packet.

'Time of Flight' is a technique used for prevention of wormhole attacks. It calculates the round-trip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up traveling further, and thus cannot be returned within the short time.

'Directional Antennas' are a good solution for wormhole detection for networks relying on directional antennas. Here, each pair of nodes determines the direction of received signals from the neighbor. If the directions of both pair match, then and then the relation is set [26]. Other types of techniques like LiteWorp, Localization and Network Visualization are also very useful in detecting wormhole attacks in wireless networks.

10. Conclusion

MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. Although fabrication of source routes (cache poisoning) is not possible in AODV while DSR is prone to it. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used. We should keep in mind that some solutions may not work well in the presence of more than one malicious node, while some require special hardware and some solutions are very expensive. So, there is still a lot of room for research in this area to provide a more secured MANET.

References

[1] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168-174, 2010

[2] Samir R. Das, Charles E. Perkins and Elizabeth M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks"

[3] Ramanarayana Kandikattu, and Lillykutty Jacob, "Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks", International Journal of Electronics, Circuits and Systems, pp. 40-45, 2007

[4] David B. Johnson, David A. Maltz and Josh Broch, " DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", http://www.monarch.cs.cmu.edu/

[5] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, "A Performance Comarison of Multi-hop Wireless Ad Hoc Network Routing Protocols", http://www.monarch.cs.cmu.edu/

[6] Hui Li and Dan Yu, "Comparison of Ad Hoc and Centralized Multihop Routing"

[7] "Mobile Ad hoc" http://www.eurescom.eu/message/messageMar2005/images/Daidalos_figure.jpg

[8] Kwan-Wu Chin, "The Microscopic Behavior of MANET Routing Protocols in Realistic Environments", 2004

[9] Sorav Bansal, Rajeev Shorey and Archan Misra, "Comparing the Routing Energy Overheads of Ad-Hoc Routing Protocols", 0-7803-7700-1/03, IEEE, pp. 1155-1161, 2003

[10] Rajiv Misra and C.R. Mandal, "Performance Comparison of ADOV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation"

[11] Kwan-Wu Chin, John Judge, Aidan Williams and Roger Kermode, "Implementation Experience with MANET Routing Protocols", ACM SIGCOMM Computer Communications Review, pp. 49-59, 2002

[12] Nor Surayati Mohamad Usop, Azizol Abdullah and Ahmad Faisal Amri Abidin, "Performance Evaluation of AODV,DSDV & DSR Routing Protocol in Grid Environment", IJCSNS International Journal of Computer Science and Network Security, pp. 261-268,2009

[13] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, "Performance Comparison of AODV,DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Journal of Scientific Research, pp.566-576, 2009

[14] "TEMPORALLY-ORDERED ROUTING ALGORITHM", http://en.wikipedia.org/wiki/Temporally-ordered_routing_algorithm

[15] Vincent D. Park and M. Scott Corson, "THE TEMPORALLY-ORDERED ROUTING ALGORITHM", http://www.ietf.org/proceedings/40/slides/manet-tora/sld001.htm

[16] N.Shanthi, Dr.Lganesan and Dr.K.Ramar,"Study of Different Attacks on Multicast Mobile Ad-hoc Network", Journal of Theoretical and Applied Information Technology, pp.45-51

[17] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan and Barber Aslam,"Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006

[18] Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research, pp. 430-443, 2009

[19] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, pp.370-380,2006

[20] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3

[21] Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks http://www.scribd.com/doc/26788447/Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks

[22] Study of Secure Reactive Routing Protocols in Mobile Ad http://www.docstoc.com/docs/30136052/Study-of-Secure-Reactive-Routing-Protocols-in-Mobile-Ad

[23] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing"

[24] Luke Klein-Berndt, "A Quick Guide to AODV Routing"

[25] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", 2003

[26] Khin Sandar Win," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008

Rutvij H. Jhaveri – Member of ISTE, Dept. In-Charge (I.T.), Sr. Lecturer, Department of Computer Engineering and Information Technology, Shri S'ad Vidya Mandal Institute of Technology, He is author of 9 research papers, with 4 papers in international conferences and international journals and 5 in national conferences in India. He is Microsoft Certified Professional and Ankit Fadia Certified Ethical Hacker. His area of interest is: Issues in Mobile Ad-hoc Networks.

Ashish D. Patel – M.E. Computer engineering, lecturer Department of Computer Engineering and Information Technology, Shri S'ad Vidya Mandal Institute of Technology, He is author of 4 research papers, with 1 paper in international conference, 1 paper in international journal and 2 in national conferences in India. He is Microsoft Certified Professional His areas of interest are data mining, network security and Algorithm analysis.

Jatin D. Parmar – M.E. Computer engineering, lecturer Department of Computer Engineering and Information Technology, Shri S'ad Vidya Mandal Institute of Technology, He is author of 5 research papers, with 3 paper in international conference and international journals and 2 in national conferences in India. He is Microsoft Certified Professional His areas of interest are Algorithm Analysis & Design, Pattern Recognition in Data Mining, Software Engineering.

Bhavin I. Shah – B.E. Computer Engineering, Lecturer, Department of Computer Engineering and Information Technology, Shri S'ad Vidya Mandal Institute of Technology, He is author of 3 research papers, with 2 papers in international conference and international journal and 1 in national conference in India. He is Microsoft Certified Technology Specialist. His research area of interest is: Issues in Cloud Computing.