An Efficient AODV Protocol and Encryption Mechanism for Group Communication and Preventing Attacks in Adhoc Networks

Sisily Sibichen, Sreela Sreedhar

Abstract— Openly available communication signals, in wireless adhoc network poses high security risk. The absence of a centralized coordination and shared wireless medium make them more vulnerable to Dos attacks. Further, closer attention should also be paid in securing the network from Grayhole and Blackhole attacks, wherein malicious nodes disrupt data transmission in the network by transmitting incorrect routing information. A realization of these enabled us to approach the subject of data security in wireless adhoc networks with a different perspective so as to have a communication route, free from all previously mentioned security threats. The purpose of this paper is to present an efficient Adhoc On-demand Distance Vector (AODV) protocol that removes the malicious node by isolating it, thereby ensuring safe and secure communication. In order to achieve this goal, the intermediate node receiving abnormal routing information from its neighbour node is programmed to consider that neighbour node as malicious. In adhoc network, as the nodes join or leave dynamically, an efficient key management mechanism is required. So, the nodes are arranged in spanning tree fashion. An efficient key exchange and encryption mechanism is presented, where each node shares secret key only with authenticated neighbours in the adhoc network to provide more security and thus avoids global re-keying operations. The proposed method aims to use two encryption techniques to forward data among the nodes.

Index Terms—Adhoc networks, AODV protocol, Authentication, Blackhole attack, Grayhole attack, RSA key exchange, Spanning tree

1 Introduction

A wireless adhoc network is a decentralized type of wireless network. It is capable of operating without the support of any fixed infrastructure and the nodes communicate directly between one another over wireless channels [1]. It is made up of multiple nodes connected by links. As the wireless channels are openly available and propagate through the air, security in adhoc networks is a major concern [4]. To provide security, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. The security goals such as confidentiality, integrity, authentication, availability and non repudiation are to be accomplished. The main advantage of adhoc network is its economically less demanding deployment.

The absence of a centralized coordination and shared wireless medium make them more vulnerable to Dos attacks on the network layer. Blackhole and Grayhole attacks are widespread attacks on adhoc networks. In Gray hole and Black hole attacks malicious nodes deliberately disrupt data transmission in the network by sending incorrect routing information [2]. In Black hole attack, the malicious node generates and propagates fabricated routing information and advertises itself
as having a valid shortest route to the destined node. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. The malicious node intercepts the packets, drops them and thus, the packets do not reach the specified destination network. Grayhole attack is an extension of Blackhole attack in which a malicious node's behaviour is exceptionally unpredictable. A node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Both attacks disturb the route discovery process and degrade network's performance [3].

In this paper, an efficient security mechanism to secure group communication and to prevent Grayhole and Blackhole attacks using AODV protocol is proposed. In this proposed mechanism, when the network consisting of multiple nodes is created, it first checks if there is any malicious nodes existing in the network. To remove the malicious nodes an advanced AODV protocol mechanism is used. Thus the malicious nodes are isolated. Any intermediate node receiving abnormal routing information from its neighbour node considers the neighbour node as a malicious node. The intermediate node appends the information about the malicious node in the route reply packet and every node receiving that reply packet then upgrades its routing table to mark the node as malicious node. When a routing request is sent, a list of malicious nodes is appended to the packet and every node receiving the packet upgrades its routing table to mark the listed nodes as malicious. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then advice other nodes not to consider the routing information received from the malicious node.

The network consists of a set of nodes. Every node has a unique id and every packet is stamped by the id of its source node. A physical network node is an active electronic device

- *Sisily Sibichen is currently pursuing masters degree program in Computer Science and Engineering: Specialization in Data Security inTocH Institute ofm Science and Technology,Ernakulam,Kerala,India. E-mail:sisily.sibichen@gmail.com*
- *Sreela Sreedhar is currently working in Computer Science and Engineering Department in TocH Institute of Science and Technology. E-mail: sreelasreedhar@gmail.com*

that is attached to a network, and is capable of sending, receiving, or transmitting content over a communication channel. This basic information is maintained at each computer node in the network. The nodes are to be organized in spanning tree topology. The spanning tree maintains security associations only with neighbouring nodes.

A modification of key management and encryption scheme, called neighbourhood key method in which each node shares secrets only with authenticated neighbours in the adhoc network is used. Key exchange occurs only between the authenticated neighbours. This avoids group re-keying [5]. Also, the time taken to exchange the key is reduced considerably as well as authentication is also increased. Whenever there is a change in the set of authenticated neighbours, a node must compute a new key and send this new key to all its authenticated neighbours. This method ensures integrity and confidentiality of application data in adhoc networks. After key exchange, the message is encrypted twice, by using neighbourhood key and message specific key. Thus the security is increased.

2 Proposed Scheme

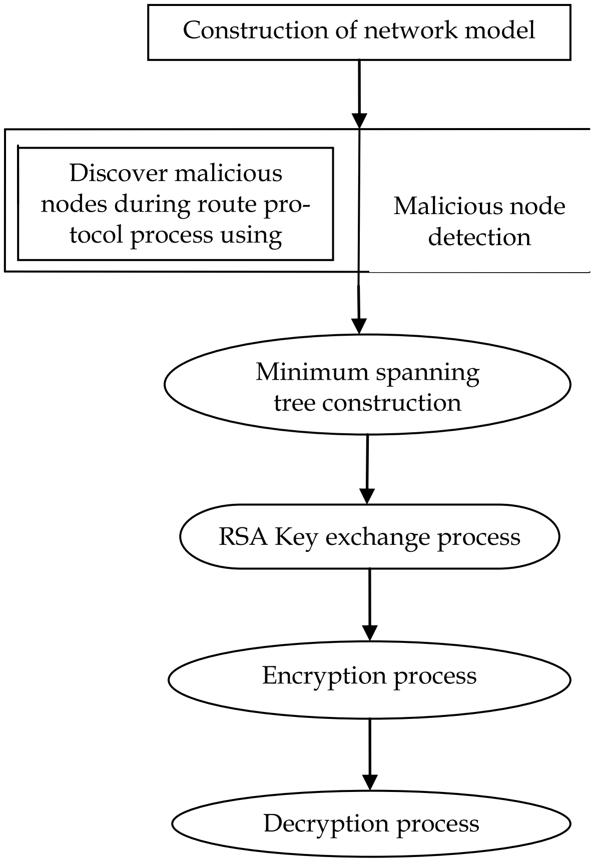

Construction of network model
Discover malicious nodes during route protocol process using
Malicious node detection
Minimum spanning tree construction
RSA Key exchange process
Encryption process
Decryption process

Fig 1: Proposed scheme architecture

3 AODV Implementation

AODV is a reactive packet routing protocol. It establishes a route from source to destination only on demand. To find routes, the AODV routing protocol uses a reactive approach. The basic message set consists of: RREQ – Route request, RREP – Route reply, RERR – Route error, HELLO – for link status monitoring.

The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table. Every node maintains a node sequence number and a broadcast id. The source node broadcasts a route request (RREQ) packet to its neighbours. The RREQ contains the following fields:
< source addr; source sequence #; broadcast id; dest addr; dest sequence #; hop cnt >

The pair < source addr; broadcast id > uniquely identifies a RREQ [6]. Whenever the source issues a new RREQ, Broadcast id is incremented. When the neighbouring node is satisfied by the RREQ, it sends a route reply (RREP) back to the source, or rebroadcasts RREP to its neighbouring nodes, after increasing the hop count. A node may receive multiple copies of the same route broadcast packet from various neighbours. The intermediate node drops redundant RREQ and does not rebroadcast, if it receives a RREQ, which has already received with the same broadcast id and source address. When RREQ travels from a source to various destinations, it establishes a forward path set up and it automatically sets up the reverse path from all nodes back to the source. A RREP contains the following fields:
< source addr; dest addr; dest sequence #; hop cnt; lifetime >

Sequence number serves as time stamps. It ensures freshness of the route. They allow nodes to compare how fresh their information to other nodes is. Whenever a node sends any kind of message it increases its own sequence number. Each node enters the sequence number of all other nodes. Higher the sequence number, fresher the route. Thus a node can choose the most accurate path. Upon receiving a RREQ packet, an intermediate node compares its sequence number with the sequence number in the RREQ packet. If the sequence number is greater than that in the packet, the existing route is more up-to-date. Else new route will be selected.

The malicious nodes causing Grayhole and Blackhole attack will always attempt to make its sequence number higher than that of any other nodes. This makes source to assume that the route which includes the malicious node might be the shortest path to destination. The source then broadcasts the packet to malicious nodes and the malicious node will drop the packet. This ensures that the packet is not reaching the destination.

It is also necessary to discover malicious nodes during the route discovery process when they pass fabricated routing information to attract the source node to send data through it. In AODV protocol, when a node receives a route reply packet (RREP), it checks the sequence number value in routing table; if it is greater than the one in the RREP, the RREP packet is accepted; otherwise it is discarded.

Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala proposed a solution for isolating malicious nodes [7]. The structures of RREQ and RREP can be modified and add a field in the routing table. In AODV, the structure of the RREQ packet contains hop count, broadcast ID, destination IP address, destination sequence number, source IP address, source sequence number and timestamp. In addition to this, a MALICIOUS_ NODE_LIST is appended to RREQ packet to notify other nodes about malicious nodes in the ad hoc network. In AODV, the structure of RREP packet contains the destination IP address, destination sequence number, hop count, source IP address, life time and timestamp; we add a flag called DO_NOT_CONSIDER to RREP to mark/identify reply from a malicious node [8]. In AODV, routing table contains the destination IP address, sequence number, hop count, next hop IP address, precursor list, time when entry expires; we add another field to this called MALICIOUS_NODE for marking a node as malicious node. Traffic conditions in an ad hoc network determine the value of a node´s sequence number and state of a node can be expressed by number of sent out RREQs, number of received RREPs and routing table sequence number; we use these three parameters to calculate a PEAK value; to detect the existence of a malicious node. Every intermediate node dynamically calculates PEAK value. Destination sequence number of the received RREP is compared with this PEAK value [9]. The PEAK value is the maximum possible value of the sequence number that any RREP can have in the current state.

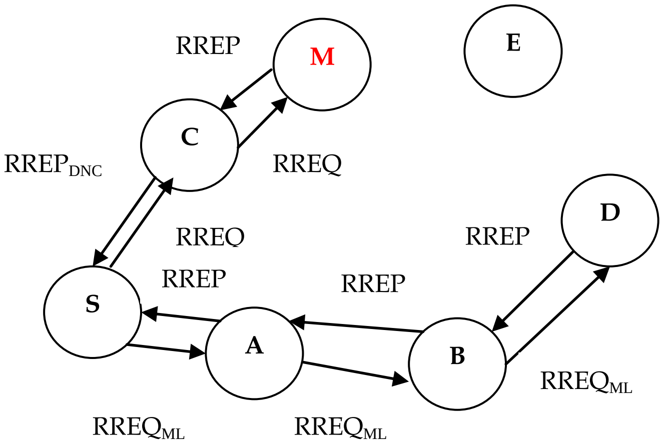


Fig 2: Route discovery process of AODV

When an intermediate node receives a RREP having sequence number higher than the calculated PEAK value, it is marked as DO_NOT_CONSIDER; the node sending RREP is marked as a malicious node in the routing table and RREP is then forwarded to the source node via reverse path. Meanwhile, each node receiving the forwarded RREP updates route entry for the malicious node. Source node sending RREQ also appends a list of malicious nodes to inform other nodes in the network about the existence of attackers. Thus, malicious nodes remain isolated from normal nodes.

4 Construction of Spanning Tree

A spanning tree is constructed by calculating the minimum distance which can cover all the nodes without forming a cycle [10]. Spanning tree construction is simple, cheap and an efficient way to connect terminals. They play a critical role in designing efficient routing algorithms. A packet can be always flooded to all members along the tree structure without loop and duplicated transmission, after a spanning tree is built to connect a group of mobile devices in the ad hoc environment. As the spanning tree maintains security associations only with neighbours, security can be considerably increased. Spanning Tree Protocol is a network protocol which establishes and maintains a spanning tree connecting a group of mobile device in the wireless ad hoc network and disables those links that are not part of the tree, leaving a single active path between any two network nodes. The distance between each node in the network is computed as follows:

$$\text{Distance } (i, j) = \sqrt{[(x_j - x_i)^2 + (y_j - y_i)^2]} \qquad (1)$$

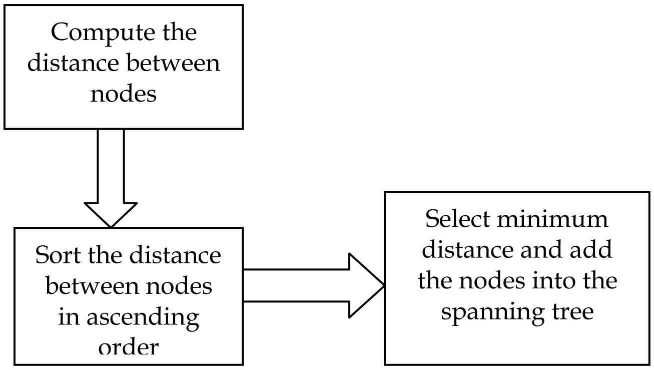

Compute the distance between nodes
Sort the distance between nodes in ascending order
Select minimum distance and add the nodes into the spanning tree

Fig 3: Construction of spanning tree

Protocol entities that execute the spanning tree protocol are referred as nodes. Each node has a logical address and a physical address. The logical address is a positive integer number, called SPT ID and set to 32 bits. The SPT ID should be unique for each node in an SPT group. When a node requires joining a spanning tree network, it starts sending and receiving beacon messages periodically. When a node requires leaving the network, it sends out a Goodbye message and stop sending and receiving beacon messages. Two nodes are adjacent when they can communicate with each other directly [11]. A spanning tree is built by locally exchanging information between nodes.

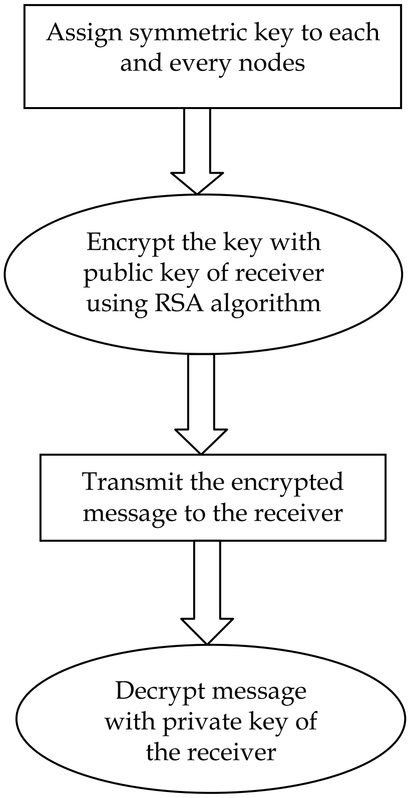
5 Authentication among Nodes

After construction of spanning tree, authentication among the nodes should be performed using public key certificates. Each node shares secrets only with its authenticated neighbours. Each node has its own certificate which has been signed by a trusted third-party. When a node receives protocol message for the first time it requests signed certificate from the other node by sending a certificate request message which includes the node’s own certificate. When a node receives a request it verifies the signature of the certificate and if valid it stores the certificate and sends certificate reply message. Verification of certificate is done by the receiving node and once they are proved to be authenticated the nodes can process each other’s protocol and application messages. In this scheme, each node performs authentication independent of and without coordination with other nodes [10].

When node B receives a protocol message from node A and if the certificate of A is unknown, node B discards the message, and sends Certification request message to A which includes B’s certificate. When A receives a request, it verifies the signature of B’s certificate and if it is valid, A stores the certificate. Node A sends Certification reply message to B that includes A’s certificate. Upon receiving the message, node B verifies the signature of A’s certificate and if it is valid, B stores the certificate. Once certificates are exchanged, the nodes exchange secret keys. These secret keys are used to encrypt or sign messages. Each node accepts messages only from authenticated neighbours.

6 RSA KEY EXCHANGE

The proposed security scheme consists of an RSA key exchange mechanism to provide security. Each node has its own symmetric key called the Neighbourhood Key. To perform encryption and decryption each node must have access to the other node's neighbourhood key. At the source, neighbourhood key is encrypted with the public key of the receiver and transmitted to the destination node. At destination, neighbourhood key is decrypted with the node’s own private key. It reduces communication overhead with the ability to have static, unchanging keys [12].


Assign symmetric key to each and every nodes
Encrypt the key with public key of receiver using RSA algorithm
Transmit the encrypted message to the receiver
Decrypt message with private key of the receiver

7 ENCRYPTION OF MESSAGE

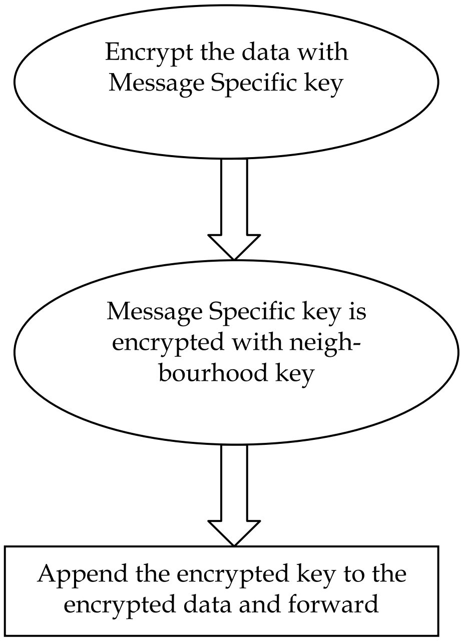

Encrypt the data with Message Specific key
Message Specific key is encrypted with neighbourhood key
Append the encrypted key to the encrypted data and forward

Fig 5: Encryption of message

Each node has its own symmetric key called neighbourhood key which is encrypted. Then, the message is encrypted using the message specific key which is the MAC address. Then, the message specific key is encrypted with neighbourhood key [9], [10]. Then, the sender appends the destination nodes ID and transmits this message to its authenticated neighbours. Source Node A creates a Message Specific Key [MKey(M)]. The message is encrypted with Message Specific Key [EMKey(M)(M)]. Then, the Message Specific Key is encrypted with A's neighbourhood key [ENKey (A) (MKey (M)]. After encryption, the Destination node's ID is appended to the Ciphertext [(ENKey(A)(MKey(M) EMKey(M)(M)) Node ID(B)].

Node A creates a Message Specific Key	MKey(M)	
Message is encrypted with Message Specific Key MKey(M)	EMKey(M)(M)	

Message Specific Key is encrypted with A's neighbourhood key	ENKey(A)(MKey(M))
	EMKey(M)(M)	

Destination node's ID is appended to the Ciphertext	ENKey(A)(MKey(M))
	EMKey(M)(M)
		B

Fig 6: Encryption steps

Two symmetric encryption algorithms are used to encrypt the message and the neighbourhood key with the message-specific key. The advantage of implementing two different encryption procedures is to make it to improve the security of the message being forwarded in the ad hoc network which is susceptible to more vulnerable attacks.

8 Decryption of Message

Encrypted message at node B	ENKey(A)(MKey(M))	ENKey(M)(M)(M)	B
If B is the intended recipient decrypt with A's neighbourhood key	DNKey(A)(ENKey(A)(MKey(M)))	ENKey(M)(M)	
Decrypt message with the obtained message key	MKey(M)	DNKey(M)(ENKey(M)(M))	
If B is not the intended recipient, ID of node C is appended	ENKey(A)(MKey(M))	ENKey(M)(M)(M)	C
Decrypt the message key with A's neighbourhood key	DNKey(A)(ENKey(A)(MKey(M)))	ENKey(M)(M)	C
Re-encrypt the message with B's neighbourhood key	ENKey(B)(MKey(M))	ENKey(M)(M)(M)	C

Fig 7: Decryption steps

At the receiver, if the appended ID matches with the node's ID, then it is the intended recipient and decryption is first performed with neighbourhood key of sending node and the plain text message is obtained. Further decryption is done with the message specific key and the original message is obtained. If the ID does not match, that node is not the intended recipient. So it re-encrypts the message with the neighbourhood key and transmits to its authenticated neighbour nodes. The procedure is repeated until destination node is found and the original message is decrypted at the destination node.

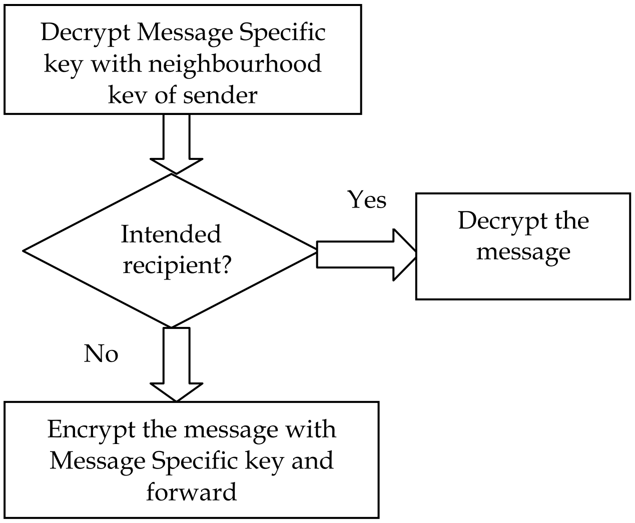

Decrypt Message Specific key with neighbourhood kev of sender
Intended recipient?
Yes
Decrypt the message
No
Encrypt the message with Message Specific key and forward

Fig 8: Decryption of message

9 Conclusion

Among various others, the Grayhole and Blackhole attacks are considered as the most dangerous attacks towards adhoc network. Even though, there exist several mechanisms for securing adhoc networks from these attacks, traditional preventive approaches in this regard have serious limitations and several disadvantages. In this paper, to provide security in group communication, nodes share a single symmetric key for encryption and decryption of messages. If a new node joins or leaves then the group key must be globally updated and distributed. This is referred to as group re-keying which is complex and needs access to a common server. Also AODV fails to remove malicious nodes during the route discovery process and therefore does not succeed to transfer all data packets to the destination under Blackhole and Grayhole attacks. Most of the traditional methods lack reliability. Also, under these attacks, the Packet Delivery Ratio (PDR), Average End-to-End Delay, Normalized Routing Overhead drops, as the number of malicious nodes increases. So a new mechanism for securing ad hoc networks has been proposed.

Whenever a network is created, an advanced version of AODV is applied first to remove the malicious nodes causing Grayhole and Blackhole attack. Then the nodes are arranged in a spanning tree fashion. Once the network is created, communication occurs only among authenticated neighbours. Further RSA key exchange is applied before encryption and decryption of messages. To improve security, encryption has been done twice. It ensures forward and backward secrecy. Whenever the topology change, new neighbourhood key is computed and is distributed to all authenticated neighbours.

In conclusion, as a result of all these mechanisms, Grayhole and Blackhole attacks can be prevented and specifically worthy of attention is the proven increase in throughput and increased Packet Delivery Ratio.

Acknowledgment

First and foremost I thank God Almighty for his blessings for completing this paper. I take this opportunity to express my gratitude to all those who have helped me in completing this work. I am also thankful to all the faculty members of Department of Computer Science and Engineering , TocH Institute of Science and Technology,Ernakulam and my friends whose co-operation and suggestion helped me a lot throughout the work.

References

[1] Vesa Kärpijoki, “Security in Ad Hoc Networks”, *Seminar on Network Security*, 2000.

[2] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, “Black Hole Attack in Mobile AdHoc Networks”, *ACMSE*, April 2004, pp.96-97.

[3] Gao Xiaopeng and Chen Wei, “A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, *IFIP International Conference on Network and Parallel Computing Workshops*, 2007, pp. 209-214.

[4] Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks”, *IEEE*, November 1999.

[5] X.B. Zhang, S.S. Lam, H. Liu, “Efficient group rekeying using application-layer multicast”, *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, (ICDCS 2005)*, June 2005.

[6] Charles E. Perkins and Elizabeth M. Royer. “Ad-Hoc On- Demand Distance Vector Routing”, *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications,* Feb.1999,pp. 90-100.

[7] Rutvij H.Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks”, *Second International Conference on Advanced Computing & Communication Technologies*, 2012.

[8] Rutvij H.Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs”, *INFOCOMP,* v. 11, no. 1, p. 01-12, March of 2012.

[9] Payal N. Raj and Prashant B. Swadas, DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET”, *International Journal of Computer Science* 2:54–59, 2009.

[10] S. Sumathy, B.Upendra Kumar, “Secure Key Exchange and Encryption Mechanism for Ad Hoc Networks”, *First International Conference on Networks & Communications*, 2009.

[11] Jorg Liebeherr, Guangyu Dong, “An overlay approach to data security in ad-hoc networks” Science Direct, Ad Hoc Networks, pp. 1055-1072, July 2006.

[12] Navita Saini, P.R. Suri, Gurpreet Singh, Sushil Pensia, “Comparative Study of Various Key Exchanging Algorithms”,*International Journal of Advances in Computer Networks and its Security*.