International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

Key Based solution for the Security Issue of Ad Hoc on Demand Distance Vector Routing Protocol in Manet

Mubeena. M[1], M.Priyanka[2], K. John Singh[3]

[1,2]*School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.*
[3]*Assistant Professor (Selection Grade), School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.*

Abstract **- Mobile communication is one of the most prominent wireless communication networks. In which a Group of mobile nodes or devices can move generously and arbitrary in an unwrap environment. The connection existing between these nodes for communication are proficient of changing their formation on a continuous basis. Mobile Ad hoc Network (MANET) is not a systematize infrastructure. The convenience is that the network can be rapidly organized. To institute the communication between the source and destination, routing protocol is used to afford the link for that communication. The most important purpose of such ad hoc network routing protocol is exact by means of well-organized path establishment between a couples of nodes so that communication may be deliver into a well-timed mode. One of the well known routing protocol for mobile ad hoc network is Ad hoc on demand distance vector (AODV) routing protocol, it invoke the route only when there is a demand, and in addition it outperforms in certain circumstances and give scalable solution to relatively large set of network topologies. This paper examines Ad hoc On Demand Distance Vector routing protocol for mobile ad hoc network and evaluate the protocol based on a set of parameters: delay, traffic, congestion, data delivery and accomplish to enforce the new approach for the improvement in Ad hoc On Demand Distance Vector to significantly reduce the entire drawback and moreover provides the efficient protection against all attacks.**

Keywords **- MANET, Ad-Hoc Networks, AODV, Security, Key Passing, Encryption**

I. INTRODUCTION

In modern era, wireless network become an important paradigm by their suppleness and effortlessness communication. Wireless networks contain a number of nodes which communicate along with others through a wireless connection. A various types of Wireless networks such as Sensor network, Mobile Ad hoc networks, cellular networks and satellite networks. Though, most of these wireless networks have controlled on infrastructures like an access point and a base station.

For this basis, Ad-hoc network with no specific infrastructures are enforced and are explained by many analysers due to their quick construction and destruction of infrastructure without any administrative server. Ad-hoc networks are independent systems consisting of routers and hosts, which are able to maintain the movable nodes and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. In Ad hoc Network, if mobiles are assigned as their nodes then it is categorized as (MANET) Mobile Ad hoc Network. Within it maintains the connectivity between nodes by wireless communication and movement of nodes from IN and OUT of topologies in unspecified moment. Mobile Ad hoc network is completely decentralized without any fixed base station, so it requires extremely flexible technology for establishing the connection. Mobile Ad-hoc Network contains collection of wireless mobiles nodes which insist to forward packets to each other and may allow them to communicate beyond direct wireless transmission range. In favour of routing the packets, a range of algorithms have been considered which are branded according to the concentrate they rely on. Many Routing protocols have been specifically designed for Mobile Ad-hoc Network.

Each protocol differs depending on the application and network architecture. The routing algorithm is one of the vital subjects of ad-hoc networks, as the network topology is changed with passion by the flow of every node. In direct to explain this issue, countless routing protocols in ad-hoc networks have been anticipated by near. Ad-hoc networks protocols are grouped into proactive and reactive type. The proactive routing protocol contains a routing table that is refreshed in every node by interchanging routing details among nodes regularly. Because of this cyclic interchanges there is a serious routing overhead. To comprehend the less overhead in ad-hoc networks, we concentrate on reactive type protocol, the most popular type that follows the source-initiated on-demand approaches.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

The on-demand protocol creates a route to a destination node only when it is necessary by a source node. Its overhead is less when compare with proactive type. Without any existing structure, it is difficult for people to distinguish the insider, outsider and attacker. Due to lack of centralization and dynamic changes in network topology certain intruders disrupt the network performance and reliability during the data transmission. Because of the attacks we need to employ some security to the network system. Security mechanism has become a critical challenge in MANET, we need to implement the mechanism to ensure the authentication, integrity and non-repudiation of the routing information of a protocol, and preventing them from being forged or disrupt. The rest of this paper is prepared as follows: Section II discusses the Problem Definitions, Section III is about the related works, Section IV describes the security goals and issues of AODV routing protocol, and Solution is proposed for the secure AODV in Section V. In section VI Simulation and result, discussion is described.

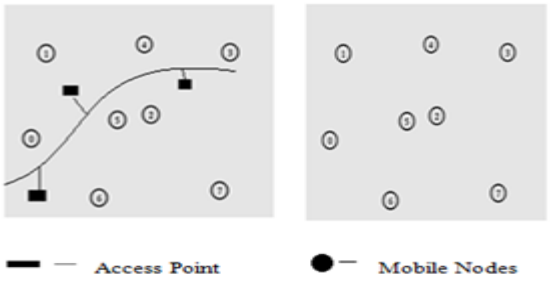


Figure 1.Wireless Network and Mobile Ad hoc Network

A *AD HOC on demand distance vector routing protocol*

Ad-hoc on demand Distance Vector routing is an involuntary routing protocol. It is deliberated for ad hoc mobile networks. AODV is skilled for both unicast and multicast routing. It is an on demand algorithm that implants routes among nodes only when there is need by source nodes. It follows these routes as long as they are required by the sources. AODV service series numbers to make sure the bloom of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV establish routes using a route request, route reply series. When a source node needs a route to a destination for which it does not already have a route, it sends a route request packet transversely the network. Nodes receiving this packet notify their information for the source node and set up rearward pointers to the source node in the route tables.

In addition to the IP address of the source node, current sequence number, and broadcast ID, the route request also contains the most current sequence number for the destination of which the source node is alert. A node receiving the route request may send back a route reply if it is the destination or if it has a route to the destination with equivalent sequence number greater than or equal to that enclosed in the rout request. If this is the case, it unicast a route reply back to the source or else, it rebroadcasts the route request. Nodes keeps the pathway of the route requests, IP address of source and broadcast ID. If they receive a route request which they have already dealt with, they dispose the route request and will not forward it.

B *Route discovery*

Ad hoc on demand distance vector protocol as the name stands it discover the route only on demand. Hence the needy node sends a request for the route by using handshake mechanism called route request and route reply. Route Request is send by source node and then procreated by intermediate nodes till the message reaches to its destination. Once the source node gets the route request it reply with a notification called Route Reply

C *Route maintenance*

After the route establishment, there should be a route maintenance section. For that we need a protocol that gives feedback about the route and to permit the route to be changed in case of any interruption because of the movement of nodes. Maintaining the established route is necessary for two main advantages, first to achieve steadiness in the network and next to minimize the overhead required in discovering new route. The discovered route is valid until the data transfer get over.

II. PROBLEM DEFINITION

MANETS are more susceptible to security attacks than agitated networks due to the open medium, briskly varying network topology, joint algorithms, short of centralized, control and short of clear line of protection. For the period of data exchange between these nodes there may be suspicious nodes, security attacks, which destruct the network act and steadiness. AODV comes under immediate routing protocol; in this scenario each node has a sequence number and each time when the link alters the sequence number get increases. The security issues are attacker either from outside the network or within the network can easily venture the network. The malicious node will be under control of the attacker and that leads to security issues.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

III. RELATED WORK

Author [1] describes the quality of service support in Mobile Ad-hoc Network .It is very problematical charge because of the enthusiastic topology, top secret resource and wireless connection characteristics. Routing protocol is very important mechanism for QOS sustain. AODV is an excellent selection for ad-hoc establishment which select a path with undersized bandwidth utilization and scalable to large population of nodes. Author [2] improved the Quality of Service of MANET and analyzed its performance with increasing number of mobile nodes. The set of connections are estranged into clusters. Each cluster contain MANET node with Cluster Head access. From one cluster to another cluster or within cluster they applied AODV routing protocol which will be loyal to ascertain the desire route for data communication. Routing regularity is improved since a collapse of one Cluster Head access does not crack all routing to outside the cluster due to use of abundant CHG. Author [3] explains about security concerns of MANET and also provided some information by assessment existing security issues which explain about how to avoid attackers and how to overcome the attacker who misuse the routing messages. Author, further described a new method called Secure Ad Hoc On-Demand Vector which provide security to AODV to protect the route discovery method by applying the security testing method. By analyzing those existing protocols, some key technique like digital signature, hash chains, etc.., can be used all together to accomplish improved secure routing protocol. Authors [4][5] describes about explicit security Issue on AODV Routing Protocol Suffering from Black hole Attack**.** Source node sends the routing information to the nasty node which essentially cannot have a path to destination node in its own routing table. It thinks that fake route reply and it ignored the message without passing to destination. Authors include the exact method to overcome the black hole attack by providing a new method called Secured AODV (SAODV). It provides an additional procedure to AODV algorithm by requesting source node to broadcast the Secured Route Request) along with random sequence number to destination. Destination checks whether Source request sequence number from two or more path are same. If so then it transfer the data in fastest path among the two and also broad cast a warning message to entire network to separate the node who send RREP in front of the two fastest routing path. Author [6] discussed about the annoyance of AODV also the contradictory situation made by the halfway nodes.

Recommended adaptation for exploring the unseen terminals in the ad-hoc network for that he propose a fare and share algorithm, in ad-hoc the network is calm until there is a need of a route, when a node need a connection that node put out a request and other nodes promote this request. There is no added traffic by enabling a mechanism called RTS/CTC to stay away from collision. RTS/CTS are the handshake system this is measured to lessen the collision. Hybrid AODV protocol is projected by Author [7], named as improved AODV. It is the compound form of the multi path and path accumulation. As the multi path is apposite to trim down the frequency of route sighting by discovering multiple paths as of source to destination and vise versa. The path addition permits to add the path discovered by multi path AODV. The main two courses that are carried out by IAODV are to turn up the route and to determine it. While correlating IAODV with AODV the IAODV can trim down the network delay and amplify the efficiency of packet deliverance. Author [8] discussed about the two crisis in AODV which are route innovation that is when the source node desires to send the data to the destination, it consult to the routing table to acquire the information concerning nodes, and send the data to subsequent hope; if legal steering information is not presented then the source node put out a Route request. The serial number in every node is amplified by one when each node sends Request. After broadcasting Route request the source node have to remain for the Reply by the destination, that's makes convinced that the information sends by the sender has reached the destination of the available path and Route maintenance. The discovered path should be maintained until the data transfer gets complete, when there is a change in MANET topology the routing table will be updated from time to time. Author [9] proposes an algorithm that helps to pass up flooding. Intend of this algorithm is to reduce the packet number in the ad-hoc network. DSDV,DSR and AODV are measured for relative study as a outcome of simulation a routing table is maintained by DSDV that contain all destination details hence it call for a large amount of memory. In DSR route catches included in each node the route is referred in this cache. It operates by sending RREQ and RREP but this is be deficient in scalability. In AODV route innovation is only on claim, and maintains the route as long as it is vibrant. It is scalable and the NS2 simulation poses it is press forward than DSR and DSDV apt to work out low bandwidth issues and the hasty change in the topology does not concern the performance.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

Author [10] the multicast route-finding protocol anticipated on the base of the unicast protocol. Multicast Ad hoc on demand distance vector protocol accredit a common multicast tree pattern and coupled all the multicast segments for all multicast cluster to convey the multicast data. A significant quality of multicast Ad hoc on demand protocol is by means of multicast succession numbers, and every multicast group has its own sequence number, which is keep up by the top ranked multicast group. By means of these sequence numbers can promise the applied routing to multicast group is always the latest. The creation of multicast direction-finding still uses the Route Request and Route Reply control message of the unicast AODV routing protocol, and joins a Multicast commencement message to confirm the multicast direction.

IV. Security Goals

The main goal of secured protocol is to have Confidentiality, Integrity, legalization and originality. Network is an open medium all the movable nodes in that medium that has a direct transmission series can acquire the data directly. We need to ensure that certain information is confidential to unauthorized users. While the data is broadcasted in open medium there is huge possibility of data get customized or destructed by attacker. We need to transmit the message as an outcome in no manner gets dishonored. Each and every node has to make sure the identity of the rake node while communicating. Without the recognition attacker can act as a peer node and thus obtain the resource and insightful information and trying to dislocate the operation of further nodes. When the source diffuses the message, it cannot be able to deny the message which was sent by it. Unconstitutional member cannot be able to act as an authorized member to discover any information.

A Security issues

- *Black-hole attack*

A black hole is a suspicious or harmful node that is under controlled by the attacker to drop all the packets by claiming that has the shortest pathway and that carries the next sequence number. In a black hole attack a spiteful node implant fake route answers to the desired node to receives, advertising itself as the straight pathway to a destination. These forged replies can be made-up to switch network traffic through the wrong node for spy, or simply to pull towards all traffic to it in order to act upon a denial of service attack by dropping the received packets.

- *Worm-hole attack*

The wormhole attacker involves the mutual aid between two malicious nodes in the network. They use tunnels between them to forward packets. Wormhole attacker always gets placed in a very powerful position and takes control of the route by claiming a shorter path. For example a Malicious node X grab routing travel at one point of the network and strike them to another tip in the network of another malicious node Y, and it shares a private declaration link with A node by claiming a shorter path with traffic nurture into the network. The connectivity of the nodes that have established routes over the wormhole link is entirely beneath the power of the two conspire attackers.

V. Solution Methodology

The proposed solution called secured cryptographic AODV (SCAODV) adds security mechanism to AODV protocol by providing some effective cryptographic mechanisms.

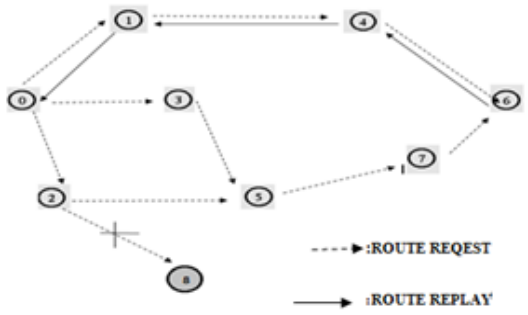


Figure 2.Malicious node accessing data.

A Secured cryptographic AODV

The secured key mechanism prevents unauthorized access from attackers. When the data is transferring in an encrypted mode only the destination node can decrypt the data because the destination node which is having the private key shared by source node to decrypt the data. So the malicious nodes which are under controlled by the attacker cannot drop the data through black-hole, wormhole attack.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

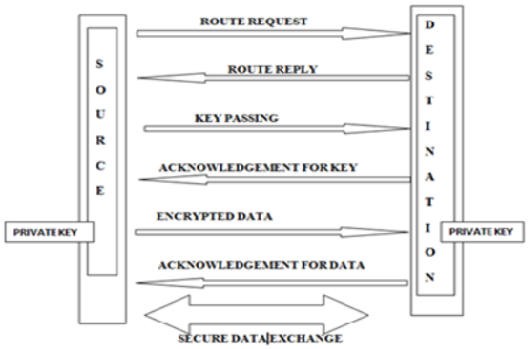


Figure 3.Handshake Mechanism For Secure Data Transmission

The proposed method implements a security mechanism so called cryptography to the existing AODV. In this the two participating nodes necessitate to select the authentication key, in order to accomplish this, RC5 symmetric keys are used. The topographically remote participating nodes need to have the same key. We implant this scenario in the route discovery stage of AODV. The source node broadcast the route request to its near stream node for the route establishment and once the route is found and got back the acknowledgement from the destination, the source node now specifically unicast the authentication key to the destination. Once the key reach the destination, source node is notified by the destination by another acknowledgement, after the handshake mechanism the message transfer starts. This mechanism provides a top level security for preventing the attacker from disrupting the information.

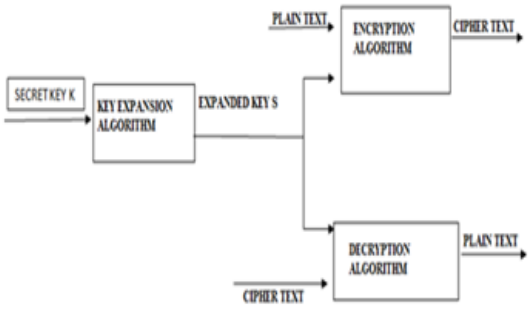


Figure 4. Flow of RC5 Key Generation and Encryption Process.

B Encryption procedure for RC5 algortihm

X=X+Ks [0];
Y=Y+Ks [1];
FOR I =1 to N do
X= ((X XOR Y) <<<Y) +Ks [2*I];
Y= ((Y XOR X) <<<X) +Ks [2*I+1];

To decrypt the encryption procedure is used in a reverse manner.

VI. Analysis And Result

Basic simulator NS2 is applied for simulation. NS2 deliberate exclusively to learn the vibrant scenery of wireless communication networks. To estimate the routine of planned scheme, we gone through a comparative study with original AODV and secure cryptographic AODV (SCAODV) protocol in the occurrence of all kind of attack like black hole attack. SCAODV is implemented as an addition to novel AODV protocol. SCAODV proposed two substitutes method to send source message to destination, the first substitute for implementation in which only destination node can send reply request. And a second substitute is by implementing the secure key passing method between sources to destination. Then we applied RC5algorithm to encrypt the data in the source and decrypt data in the destination node using the key.

A Simulation results for AODV

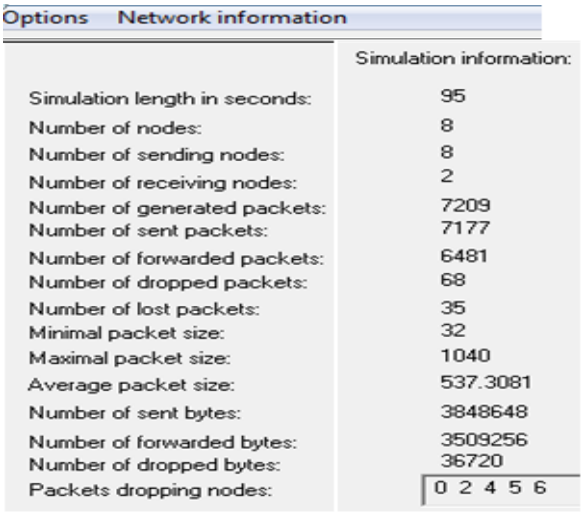


Figure 5. Simulation Information

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

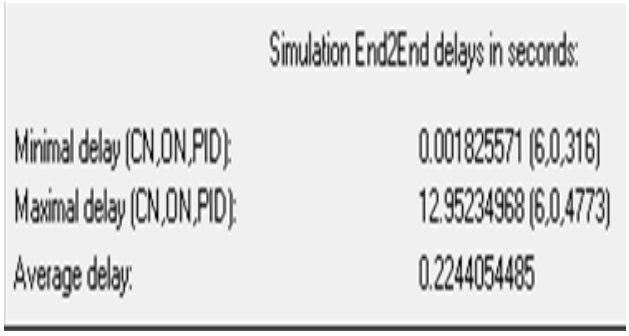


Figure 6. Simulation end to end delay in seconds

B Performance metrics of AD HOC on demand distance vector

- *Packet delivery fraction*

The packet delivery fraction produced the percentage value of data packets which sender transferred and the receiver received packets. The number of packets sent by the source and number of packets received by receiver were supposed to be match.

- *Packet loss*

The percentage of data packets missed during the transmission process.
Packet loss= (Number of packets sent) - (Number of packets received

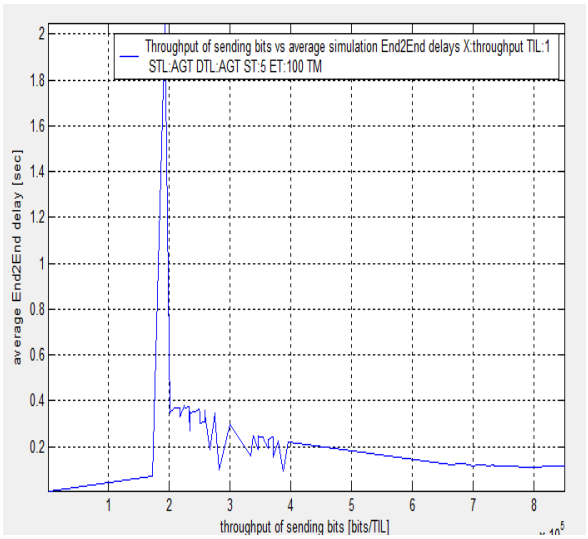
TABLE 1
SHOWS THE PACKET DELIVERY

PROTOCOL	NO OF PACKETS SENT	NO OF PACKETS RECEIVED	PACKET DELIVERY FRACTION IN %	PACKET LOSS
AODV	3580.0000	3543.0000	98.966480	37

- *Throughput*

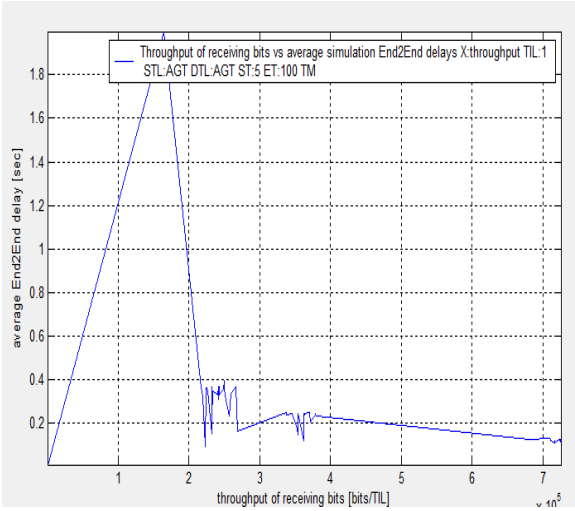
The amount of successful data transferred over the given period of time which is expressed in bits (kilobits) per second. Number of sent data packets =Number of received data packets.

GRAPH 1
THROUGHPUT OF SENDING BITS VS AVERAGE END TO END DELAY



Both the graph shows the exact result for throughput of sending and receving ackets are not equal and also produce less possiblities of congestion

GRAPH 2
THROUGH PUT OF RECEIVING BITS VS AVERAGE END TO END DELAY



International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

Screen shots for RC5 encryption and decryption

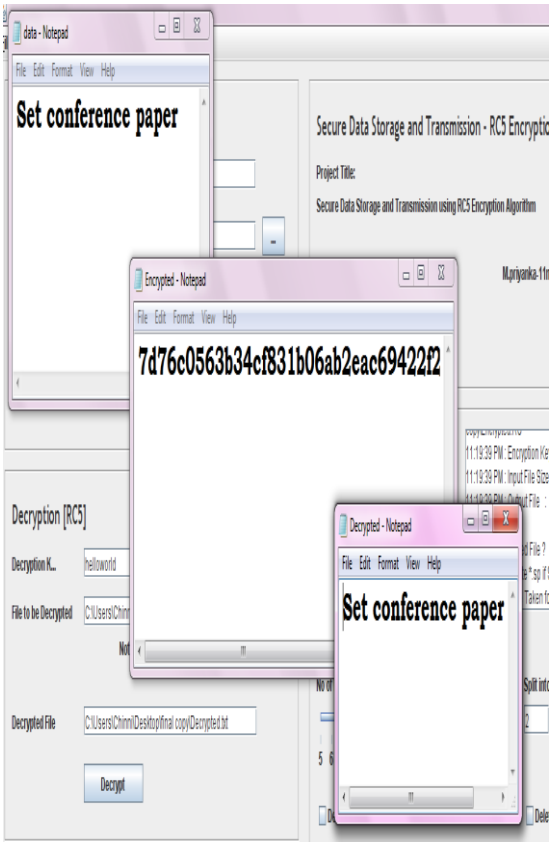


FIGURE 7. ENCRYPTION AND DECRYPTION PROCSS

VII. CONCLUSION

The Secured Cryptographic AODV protocol for MANET is presented in this paper. This protocol uses a secured key mechanism in opposition to all security attacks and to deliver secure data in MANET, The simulation result state that the proposed protocol gives higher security and may have less packet drops and throughput.

REFERENCES

[1] Royer E.M, Perkins C.E. "Ad-hoc on-demand distance vector routing". Proceedings on the 2nd IEEE Workshop in Mobile Computing Systems and Applications ,1999, pp.90-100.

[2] Ashish Bagwari, Raman Jee, Pankaj Joshi, Sourabh Bisht, "Performance of AODV Routing Protocol with Increasing the MANET Nodes and Its Effects on QoS of Mobile Ad Hoc Networks",2012 International Conference on Communication Systems and Network Technologies, pp.320-324.

[3] J Viji Gripsy, Dr Anna Saro Vijendran. "A Survey on Security Analysis of Routing Protocols". Global Journal of Computer Science & Technology on April 2011, Volume 11 Issue 6 Version 1.0, pp.1-7.

[4] K.Lakshmi, S.Manjupriya, A.jeeva Rathinam, K.Ram, K Thilagam**. "**Modified AODV Protocol against Black hole Attacks in MANET".2010,Proceeding on International Journal of Engineering and Technology,Vol.2,Issue-6, pp.444-449.

[5] Security Issue On Aodv Routing Protocol Suffering From Black hole Attack**.** Mrs. Kritika Taneja, Asst. Professor, Manav Rachna .International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 1, Issue 7, September 2012.

[6] Teena Arora, Parminder Singh, Sandeep king kang. "Performance Evaluation and Improving Bandwidth Utilization of AODV by Finding Hidden Terminals in Wireless Networks", on International Journal of Computer Science and Telecommunications, Volume 2, Issue 6, September 2011, pp.41-45.

[7] Yan Bin, Yang, Hong Bin, Chen, "An improved AODV routing protocol for MANETs", Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing, 2009, pp.2918-2921.

[8] Zhu Qiankun, Xu Tingxue, Zhou Hongqing, Yang Chunying, Li Tingjun. "A mobile Ad Hoc Networks Algorithm Improved AODV protocol", on International Conference on Power Electronics and Engineering Application. Procedia Engineering 23 -2011, pp 229 – 234.

[9] Geetam S.Tomar,Manish Dixit & Shekhar Verma."AODV Protocol with Selective Flooding**."** 2009 International Conference of Soft Computing and Pattern Recognition.

[10] Elizabeth M. Royer, Charles E. Perkins. "Multicast Ad Hoc On-Demand Distance Vector Routing Protocol**"**Proceeding on Mobile Ad Hoc Networking Working Group and INTERNET DRAFT University of California, Santa Barbara 15 July 2000.

[11] Rivest,R. L. (1994). "The RC5 Encryption Algorithm". Proceeding of the second International Workshop on Fast Software Encryption (FSE)-1994, pp.86-96.