Enhanced Security in Mobile Adhoc Networks by using ECC Cryptography Technique

A. Mohamed ILeeyas[1] M. Balaji[2] A. N. Vinoth[3]
[1, 2]ME (CSE) Student [3]M. E. (Soft Engg)
[1, 2]Student Ranippettai Engineering College, Walajah, Vellore
[3]Rajalakshmi Engineering College, Thandalam, Chennai

Abstract---A mobile ad hoc network (MANET) is a special type of wireless network consisting of a collection of nodes capable to communicate with each other without help from a network infrastructure. Due to its nature, providing security in this network is challenging. Because MANET has no any pre-existing fixed structure and mobile nodes sends packets to the destination nodes directsly or via the neighbouring nodes, it is of potential security concern because neighbour nodes cannot be trusted, While the routing aspects of mobile ad hoc networks (MANETs) are already well understood, and the research activities about security in MANETs are still at their beginning. In this paper, we propose an effective security Ad hoc On Demand Distance Vector (AODV) algorithm called ES-AODV to enhance the data security. And also we implement a technique using Elliptic Curve Cryptography (ECC) algorithm where the information is secured while passing through the nodes. Only the destination would be able to decrypt the data. This ensures that the finally received data has integrity. This protocol is energy efficient and uses low memory as we use the concept of Elliptic Curve Cryptography (ECC). Finally we analysing performance comparison of AOMDV with AODV using ns-2 simulations. Simulation results show that our algorithm provides a reasonably good level of security and performance.

Keywords: Mobile Ad Hoc Network, AODV, AOMDV, ECC, Malicious node, Secure Routing.

I. INTRODUCTION

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other.

The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems. The difference between Infrastructure and Infrastructure less Network Architecture as shown in figure (1.1)

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure.

They offer quick and easy network deployment in situations where it is not possible otherwise

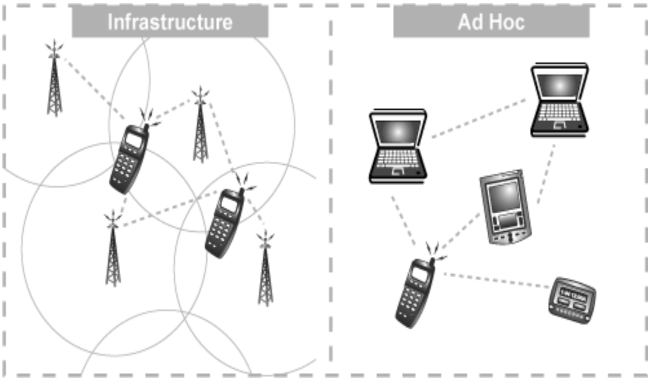

Fig. 1: Infrastructure and Infrastructure less Network Architecture.

Ad-hoc is a Latin word, which means "for this or for this only." Ad-hoc networks are temporary network. They do not need any external infrastructure like base stations and physical wires.

A mobile ad hoc network (MANET) is a wireless network that uses multi-hop peer-to-peer routing instead of static network infrastructure to provide network connectivity as shown in below figure (1.2).

Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. [1]

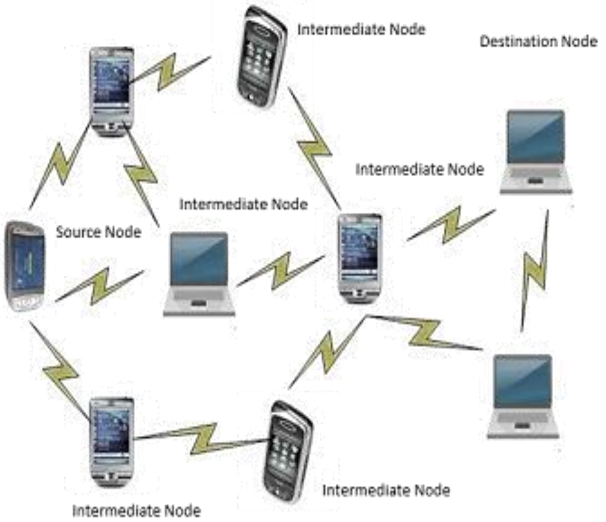

Fig. 2: Typical Architecture Diagram for Mobile Adhoc Network (MANET).

A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. [1]

The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet. [1]

Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we can imagine a group of peoples with laptops, in a business meeting at a place where no network services is present. They can easily network their machines by forming an ad-hoc network. This is one of the many examples where these networks may possibly be used.

Most of the research so far has been done in the area of routing protocols [1-4], although in recent year's security issues have also been explored. Although the basic security goals and requirements of an ad hoc network are very similar to those of a wireless network, some inherent characteristics of the former make security issues more challenging. These include absence of infrastructure, high probability of node compromise, frequent and dynamic topology change and low level of trust among the nodes.

Issues in Ad Hoc Wireless Networks [11]:

- Medium Access Scheme
- Routing
- Multicasting
- Transport Layer Protocol
- Pricing Scheme
- QoS provisioning
- Self-Organization
- Security
- Energy Management
- Addressing and Service Discovery
- Scalability
- Deployment Considerations

In this paper, we propose an effective security algorithm called ES-AODV in ad hoc wireless networks. The overall goal of this algorithm is to provide a secure solution for communication in ad hoc network applications. This protocol will be able to find a trusted end- to-end route free of any malicious entity, effectively isolating any node trying to inject malicious information into the network. And also we implement a technique using Elliptic Curve Cryptography (ECC) algorithm where the information is secured while passing through the nodes. Only the destination would be able to decrypt the data. This ensures that the finally received data has integrity. This protocol is energy efficient and uses low memory as we use the concept of Elliptic Curve Cryptography (ECC). Finally we analysing performance comparison of AOMDV with AODV using ns-2 simulations.

II. RELATED WORK

Routing protocol intrusion detection has also been studied as a mechanism for detecting misbehaving routers [4]. Mobile agent based mechanism is used in [5] to detect the intruders. And we compared some routing protocol algorithms in all aspects. AODV is the best routing protocol among it and we identified it’s the algorithm to find the intrusion in network and it can provide better routing for all the nodes by finding shortest path comparatively with other many different nodes.

Few security schemes for internal attacks are proposed for ad hoc networks. Yonguang Zhang and Wenke Lee [6] present a new intrusion detection and response mechanism for wireless ad hoc networks. [7] Present a hierarchical framework and key distribution algorithms for dynamic environment, with a focus on how keys and trust relationships are transferred when users move between so called "areas" in the hierarchy.

Behavioral Study of MANET Routing Protocols Amandeep Makkar, Bharat Bhushan, Shelja, and Sunil Taneja[8], In this paper, behavioral study of different MANET routing protocols viz. Optimized Link State Routing (OLSR), Destination Sequenced Distance vector (DSDV), Dynamic Source Routing (DSR), Adhoc On-demand Distance Vector (AODV) and Temporary Ordered Routing Protocol (TORA) protocols, have been carried out so as to identify which protocol is most suitable for efficient routing over Mobile Adhoc NETwork (MANET).

Trust Routing in MANET for Securing DSR Routing Protocol, Sultan Almotiri and Irfan Awan [9] In this paper, they design a novel secure routing protocol for mobile ad hoc networks (MANETs), called trusted dynamic source routing (TDSR) which extends the widely used DSR routing protocol and employs the idea of trust network connect (TNC) to protect routing behaviors. In the TDSR, trust among nodes is represented by trust score, which consists of direct trust and indirect trust. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes.

Security in Mobile Ad-Hoc Networks Using RSA Method, B.Lehane and L.Doyle, [10] In this paper presented a Mobile Ad-Hoc Network (MANET) which securely transmits Audio data. Even though studies on network security has been done before, secure transmission of audio has not been given much importance since both audio and Ad-Hoc network are both complex to handle. So some simple and efficient methods are required to encrypt Audio data. We aim to provide double security by encrypting and decrypting the audio at each node in the route using stream ciphering method. Key for encrypting the audio at the transmitter is generated by Fast Anti-Random Approximate (FARA) method.

III. THE PROPOSED ALGORITHM

A. *Ad Hoc On-Demand Distance Vector (Aodv)*

The AODV Routing Protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the RouteRequest packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RouteRequest.

The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination. The connection setup delay is lower.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches. Each route entry keeps track of certain fields. Some of these fields are:

1) Destination IP Address: The IP address of the destination for which a route is supplied
2) Destination Sequence Number**:** Destination sequence number associated to the route
3) Next Hop: Either the destination itself or an intermediate node designated to forward packets to the destination
4) Hop Count: The number of hops from the Originator IP Address to the Destination IP Address
5) Lifetime: The time in milliseconds for which nodes receiving the RREP consider the route to be valid
6) Routing Flags: The state of the route; up (valid), down (not valid) or in repair

B. *Adhoc On-Demand Multipath Distance Vector (Aomdv)*

Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) protocol is an extension to the AODV protocol for computing multiple loop-free and link-disjoint paths. The routing entries for each destination contain a list of the next-hops along with the corresponding hop counts. All the next hops have the same sequence number. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination. Each duplicate route advertisement received by a node defines an alternate path to the destination.

AOMDV can be used to find node-disjoint or link-disjoint routes. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. The advantage of using AOMDV is that it allows intermediate nodes to reply to RREQs, while still selecting disjoint paths. But, AOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs those results are in longer overhead.

C. *Elliptic Curve Cryptography (Ecc)*

An elliptic curve is defined by an equation of the form y2 = x3 + ax + b, where a and b are arbitrary constants. An example of an elliptic curve is shown in Figure (3.1).

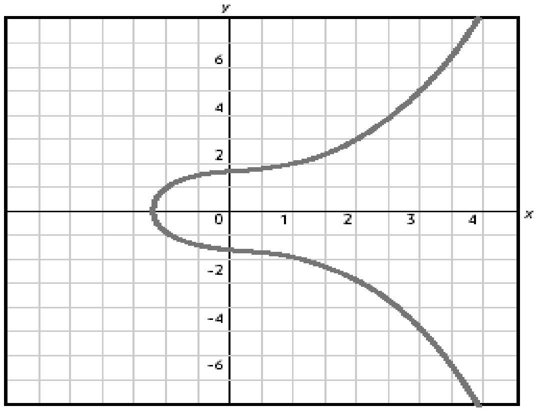

Fig. 3: Basic Elliptic Curve

Advantages of ECC

- Smaller Key Size
- Reducing Storage
- 256-bit ECC public-key provide comparable security to 3072-bit RSA public key

IV. System Design

A. *Proposed System*

To solve security issues in MANET in the existing system, First, We approach ECC algorithm is being used for encryption and decryption. Therefore communication is secured as the data cannot be viewed while it passes through the intermediate nodes. Any node in between, which tries to read this information will not be able to do so because, the information will be encrypted using ECC.

Second, AODV routing protocol is used for transmission of data. It is a reactive protocol that requests the route only when it needs. It does not require nodes to maintain routes to the destination that are not communicating.

Finally the impact of a selfish node on the network performance has been thoroughly analyzed and the choice of AOMDV over AODV has been validated through simulation results.

The special advantage in the proposed system use of ECC algorithm for encryption and decryption Hence communication is secured and no node in between can read or views the data. The keys to encrypt and decrypt the data are only known to the source and the destination, respectively.

B. *Selfish Node Analysis*

The fact that security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. One of the different kinds of misbehavior a node may exhibit is selfishness. A selfish node wants to preserve own resources while using the services of others and consuming their resources. One way of preventing selfishness in a MANET is a detection and exclusion mechanism.

This project presents the simulation results that show the negative effects which selfish nodes cause in MANET. A simulation was performed in NS2 with mobile nodes. Simulations involved 25 nodes and the number of packet dropping nodes was increased gradually from 8 to 15. Three parameters were analysed, viz. Packet Delivery Ratio, Average Throughput and End to End Delay.

C. *Multipath Analysis*

In this Multipath Analysis part, it is validated why AOMDV has to been chosen over AODV. In addition to choosing AOMDV, a scheme has to be incorporated to understand the discrepancies between the IP layer topology and Physical layer topology. Multipath discovery is done through an iterative method in which the shortest paths are found one after the other, removing the links of the path after it is done.

D. *Data Security*

The data security ensures secure transfer of data from the source node to destination node. This module includes ECC key generation where the public and private key pairs for the participating nodes needs to be generated. Therefore communication is secured as the data cannot be viewed while it passes through the intermediate nodes. Any node in between, which tries to read this information will not be able to do so because, the information will be encrypted using ECC.

V. Simulation Results

In this section, we first describe the simulation environment used in our study. Then we discuss the results in detail.

Simulation Environment

Our simulations are implemented in Network Simulator (NS-2) [13] from Lawrence Berkeley National Laboratory (LBNL) with extensions for wireless links form the Monarch project at Carnegie Mellon University.

Parameter	Value
Topology Area	600 x 600m
Number of Nodes	25
Node Transmission Range	100m
Total Simulation Time	100s
Pause Time	1s
Speed	5,10,15 m/s

A. *Performance Analysis of Selfish Node*

The Packet Delivery Ratio (PDR) has been highly affected by the presence of malicious packet dropping nodes. The PDR drops with the increase in the number of packet dropping nodes.

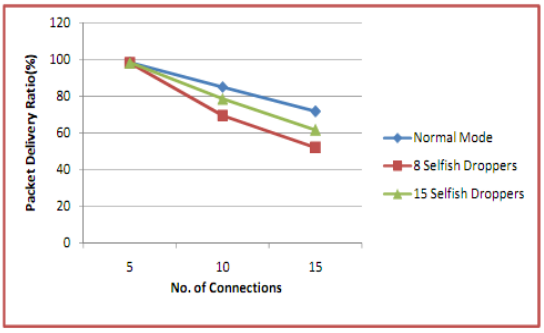

Fig. 4: (a) Packet Delivery Ratio of AOMDV in the presence of selfish nodes

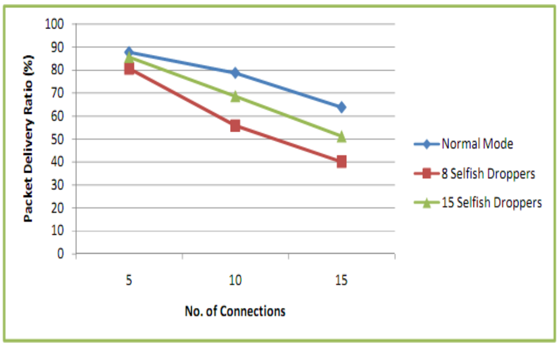

Fig. 4: (b) Packet Delivery Ratio of AODV in the presence of selfish nodes

The average throughput of the system is also affected with the increase in the number of packet dropping nodes.

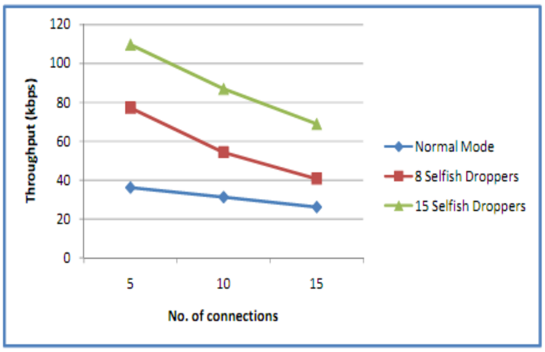

Fig. 4: (c) Average Throughput of AOMDV in the presence of selfish nodes

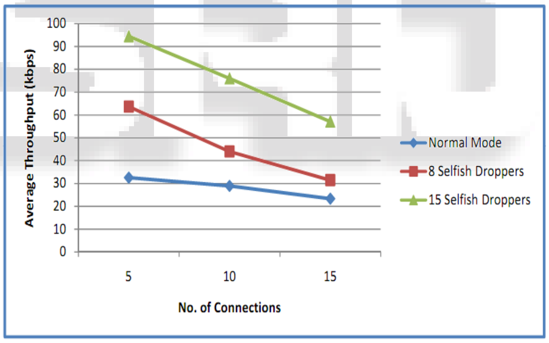

Fig. 4: (d) Average Throughput of AODV in the presence of selfish nodes

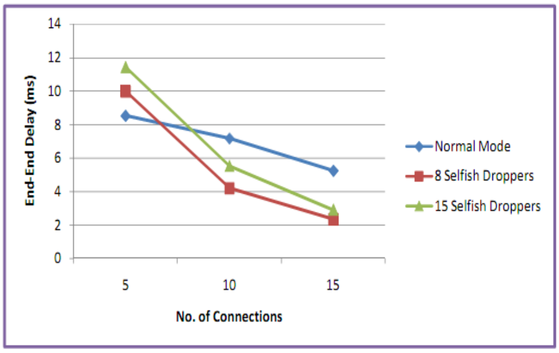

Fig. 4: (e) End to End Delay of AOMDV in the presence of selfish nodes

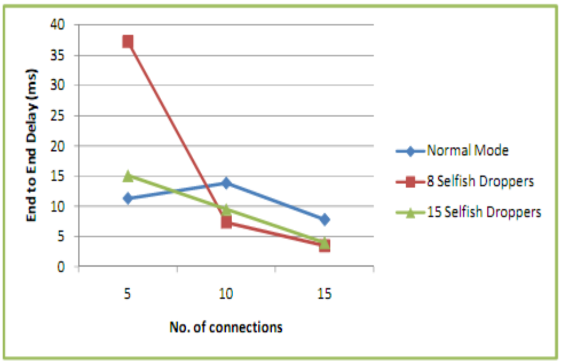

Fig. 4:(f) End to End Delay of AODV in the presence of selfish nodes

B. *Performance Analysis of Multi Path Analysis Module*

A performance analysis has also been performed to highlight the performance of AODV and AOMDV.

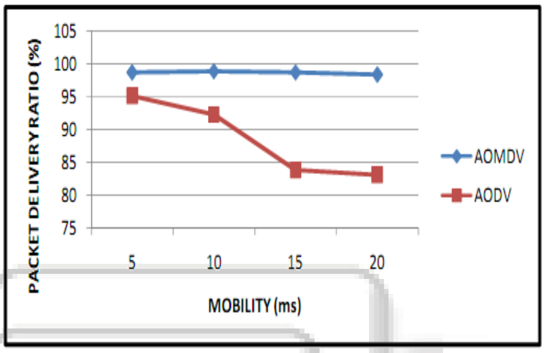

Fig. 5 (a): Packet Delivery Ratio for 5 CBR connections

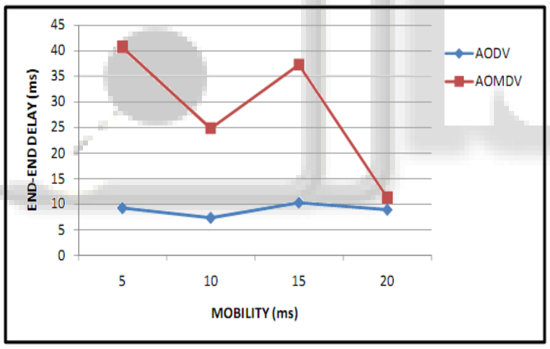

Fig. 5(b): End to End Delay for 5 CBR connections.

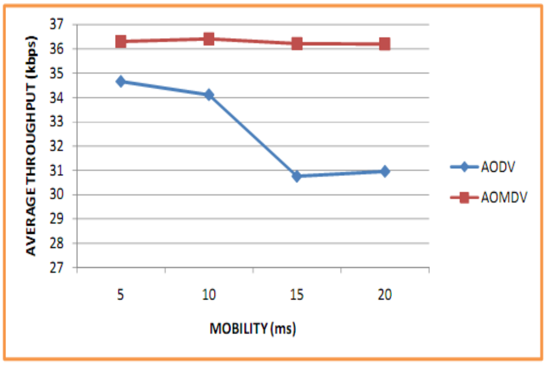

Fig. 5(c): Average Throughput for 5 CBR connections

VI. Conclusions

In this paper, we proposed an efficient security algorithm ES-AODV to enhance the security in ad hoc wireless networks. At the end of the simulation run, trace-output files are created and they have been analysed using awk and perl scripts to obtain performance graphs. Selfish node analysis illustrates the degradation in network throughput and packet delivery ratio. Multipath routing analysis proves that AOMDV performs better than when it comes to packet dropping and packet delivery, though it's routing overhead and end-end delay is comparatively higher. Also Packet dropping behaviour has been successfully simulated in ns2. Encryption and Decryption using Elliptic Curve Cryptography has also been implemented by creating custom agents mudp and mudpsink, which carry actual data.

References

[1] D. Kim, J. Garcia and K. Obraczka, "Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate", IEEE Transactions on Mobile Computing. Vol 2, no 2, 2003, pp.161-173

[2] www.isi.edu/nsnam/ns/tutorial Marc Greis tutorial on ns2

[3] David B. Johnson and David A. Maltz. "Dynamic source routing in ad hoc wireless networks", Mobile Computing, Kluwer Academic Publishers. 1996 pp.153–181, 1996.

[4] M. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols", ACM Wise, 2002.

[5] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," ACM Mobile Networks and Applications (MONET) J., Vol. 9, no. 5, pp. 545-556, sept. 2002.

[6] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad hoc networks. In 6th International Conference on Mobile Computing and Nerworking (MOBICOM'OO), pages 275-283, June 2000.

[7] Charles E. Perkins, Elizabeth M. Belding-Royer and Ian D. Chakeres. "Ad Hoc on-Demand Distance Vector Routing" Mobile Ad Hoc Networking Working Group, Internet Draft, Oct 2003.

[8] Amandeep Makkar, Bharat Bhushan, Shelja, and Sunil Taneja "Behavioral Study of MANET Routing Protocols" International Journal of Innovation, Management and Technology, Vol. 2, No. 3, pp. 210-216, June 2011

[9] Sultan Almotiri and Irfan Awan "Trust Routing in MANET for Securing DSR Routing Protocol" ISBN: 978-1-902560-24-3 © 2010 PGNet

[10] B. Lehane, L. Doyle, and D. O'Mahony, Shared RSA Key Generation in a Mobile Ad Hoc Network, Proceedings of IEEE Military Communications Conference (MILCOM), Vol.2, pp.814–819, 2003.

[11] William Stallings (2010) [Book], "Cryptography and Network Security".

[12] Manoj, B.S. and Siva Ram Murthy, C. (2004) [Book], "Ad Hoc Wireless Networks: Architectures and Protocols".

[13] NS, The UCB/LBNL/VINT Network Simulator (NS), http://www.isi.edu/nsnam/ns/, 2004.

.