International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.2, February 2013 DOI:10.15693/ijaist/2013.v2i2.1-7

Comparative Analysis of AODV and Trusted AODV (TAODV) in MANET

Mrs. P.VIGNESWARI[1],ANUSHA. R[2], PREETHI.D[3]NANDHINI. V[4] , JAYASHREE.R[5]

[1]ASSISTANT PROFESSOR, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

[2], [3], [4], [5]U.G.SCHOLARS, IV YEAR, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING ,

AVINASHILINGAM INSTITUTE OF HOME SCIENCE AND HIGHER EDUCATION FOR WOMEN,

FACULTY OF ENGINEERING,

COIMBATORE.

***Abstract* - The nature of self-organization and the limitation of individual resources, MANET always confront security and selfishness issues. In this paper, we design trusted routing protocols using trusted frame works and intrusion detection system (secure protocol) for MANET called TAODV. Our results show that the cumulative utilities of cooperative nodes are increased steadily. The Trust Scheme evaluates the behavior of all nodes by establishing a trust value for each node in the network that represents the trustworthiness of each one thereby identifies and eliminates the malicious nodes. It also observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboring nodes, and the past activity of the node. To make better security in this phase we propose multi path communication and data encryption using key verification. The multi path communication can be carried out among trust nodes only.**

Keywords: MANET, AODV, Security,
Trusted AODV.

I.INTRODUCTION

A Mobile Ad-hoc network (MANET) is a network that has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. These type of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses number of challenges in ensuring the security of communication, something that is not easily done as many of the network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (Example: Low power consumption, Low processing load).

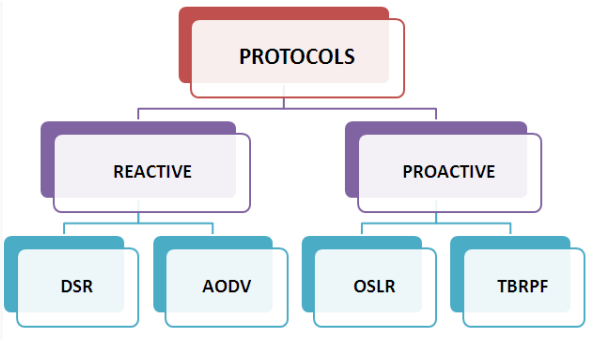


Fig I:Classification Of Protocols

A major issue in Mobile Ad-hoc network is "SECURITY". The security mechanism for MANET, must require low computational complexity and small number of appended messages to save the node energy, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. Two approaches in protecting Mobile Ad-hoc networks.

Proactive Protocol: Traditional distributed shortest-path protocols, based on periodic updates. It has high routing overhead and also prevents an attacker from launching attacks through various cryptographic schemes.

Reactive Protocol: Seeks to detect security threats and react accordingly. Discover routes when needed. Source-initiated route discovery, because of this we go for reactive protocol.

The two types of reactive protocol are DSR and AODV. Dynamic Source Routing (DSR) and Ad-Hoc On Demand Distance Vector Routing (AODV) both are routing protocols for wireless mesh/ad hoc networks. Both are demand-driven

protocols which form a route on demand when a transmitting computer desires a route. The DSR is based on source routing in which all the routing information such as is maintained at the mobile nodes. The DSR computes the routes and also updates them. The main drawbacks in this are:

1. Maintains additional table entries, causing a larger memory overhead.
2. Not capable of handling congestion.
3. Does not remove the broken path, hence time consuming.
4. Routing packets are large.
5. Relatively small network diameter.

Therefore we go for AODV protocol. The AODV uses a combination of a DSR and DSDV[6] mechanism. It uses the route discovery and route maintenance from a DSR and hop-by-hop routing, periodic advertisements, sequence numbers from DSDV. The AODV easily overcomes the counting to infinity and Bellman Ford problems, and it also provides quick convergence whenever the ad hoc network topology is altered.

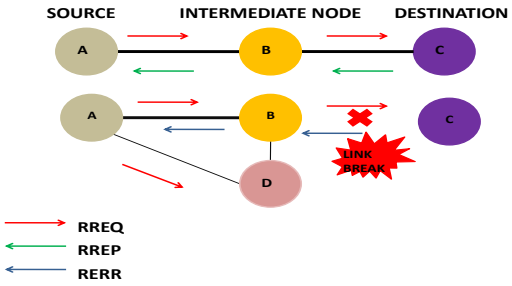
In our work to be described in the thesis, we focused on designing a secure routing mechanism for MANET in a self-organized way instead of using centralized servers since these centralized servers or trusted parties make the network more controllable but they destroy the self-organizing nature of MANET and reduce the network scalability. Our solution is introducing the idea of "trust" to solve this problem. Based on this trust model, we design our secure routing protocol for MANET according to Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called TAODV (Trusted AODV), has several salient features:

(1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them;
(2) A node which performs malicious behaviors will eventually be detected and denied to the whole network;
(3) System performance is improved by avoiding requesting and verifying certificates at every routing step.

II.AODV Routing Protocols

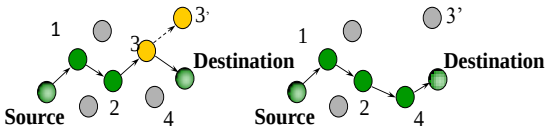
A. Secure Ad-hoc on Demand Distance Vector Routing (SAODV):

SAODV is an extension to AODV. It uses asymmetric cryptography to secure AODV's routing messages. SAODV uses Digital Signatures to protect the non-mutable data in the RREQ and RREP messages. The four basic operations performed for the Route Establishment are 1.Route Discovery 2.Route Request 3.Route Reply and 4.Route Maintenance. Before entering the network, each node obtains a public key certificate from a trusted certificate server. There are End-to-end authentication between source and destination and Hop-to-hop authentication between intermediate nodes. Hash chains are used in SAODV to authenticate the hop count of the AODV routing. Source broadcasts signed RDM (Route Discovery Message)[1] along with its own certificate. RDM contains the source IP address, along with a source-specific nonce (to detect duplicates).



FigII.A.1:Represents route discovery, route request, route reply and route error

First hop adds its own signature and certificate. Each hop verifies signature of previous hop and replaces it with its own signature also adds a reverse route to source. Destination also verifies the source signature. In Route Reply the destination sends back a signed reply (RRM) to the first RDM. The discovered Route may not be the shortest, but is the "quickest". Route Maintenance Nodes send signed error messages (RERR) to indicate link breaks, and packets arriving on deactivated paths.



FigII.A.2: Represents route maintenance

Hop count authentication by using hash chains is not perfect since a malign node might forward a message without increasing the hop count. Tunneling attacks are not solved by SAODV. The processing power requirements of SAODV should be reduced due to the use of asymmetric cryptography.

B. Adaptive SAODV (A-SAODV):

Adaptive mechanism that tunes its behavior for optimizing the performance of routing operation is called Adaptive SAODV (A-SAODV) which is a multithreaded application. Cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other message and other thread to all other functions. Each node has to maintain a queue length field for all neighboring node along with the list of neighborhood nodes which they may update and exchange with the help of hello message periodically.

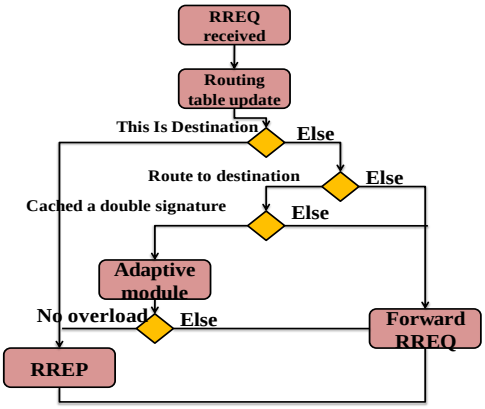


Fig II.B:Flowchart Representing Adaptive SAODV

When an intermediate node receives a RREQ and finds that it has the valid route to the destination, it check its time to leave field(TTL) then simply forwards RREQ only to this neighboring node, otherwise, it reply to the source using method involved in SAODV.

If RREQ packet is less than the TTL_threshold value the request packet is simply forwarded to all neighboring nodes This may significantly reduce the queue length of any intermediate node. The prototype also maintains a cache of latest signed and verified message in order to avoid signing and verifying the same message twice.

C. Security Aware Ad-hoc Routing (SAR):

SAR is an approach to routing that incorporates security levels of nodes into traditional routing metrics. The goal of SAR is to characterize and explicitly represent the trust values and trust relationships associated with ad hoc nodes and use these values to make routing decisions. The route discovery mechanism will then find nodes that match particular security attributes and trust levels. Only nodes that provide the required level of security can generate or propagate route requests, updates, or replies. If the node cannot provide the required security, the RREQ[8] is dropped. However SAR is able to find a route with guarantee of security. If one or more routes that satisfy the require security attributes exist, SAR will find the shortest such route. If all the nodes on the shortest path between two nodes can satisfy the security requirements, SAR will find routes that are optimal. Timeliness, ordering, authenticity, integrity, confidentiality are some of its properties.

The main drawback in SAR is it requires excessive encryption and decryption.

D. Reliable Ad-hoc on Demand Distance Vector Routing (RAODV):

RAODV also uses RRDU and RRDU_REP[6] to help discover the path and for reliability maintenance. Path discovery in RAODV[3] can be thought of as consisting of two phases. Phase I is same as that in AODV. That is, when a node wishes to communicate with another node it looks for a route in its table. If a valid entry is found for the destination it uses that path else the node broadcasts the RREQ to its neighbors to locate the destination. The process continues until either the destination or an intermediate node with a fresh route to the destination is located. At each intermediate node, a reverse path is created for the source. The source receives RREPs from all these paths In Phase II the source node sends an RRDU packet to all the nodes from which it gets the RREPs. Now since replies to RRDU, i.e. RRDU_REP packets are generated only by the destination and there is no impersonation, the source node will receive a unique RRDU_REP and the path discovery is completed.

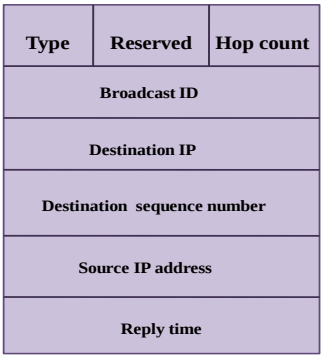


Fig II.D:Routing Table of RAODV

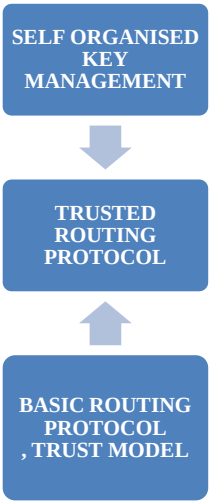
III. PROPOSED SYSTEM

The basic idea is to build a trust model that provides nodes with a mechanism to evaluate the trust of its neighbors. A node assigns a so-called trust level for each neighbor, which represents how trustworthy each neighbor is. We have improved the performance of routing protocol against the malicious attacks. Since a malicious node behaves in abnormal ways, this mechanism proposes observing nodes behavior such as nodes' mobility, and avoiding communication through these nodes which may lead to more secure routing. This method identifies malicious paths between the source and the destination nodes. The Trust Scheme evaluates the behavior of all nodes by establishing a

trust value for each node in the network that represents the trustworthiness of each one. It observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboring nodes[5], finding the malicious node and calculate these parameters to determine which nodes are misbehaving in the network and performance is improved by avoiding requesting and verifying certificates at every routing step.

We assume that:
a. Each node in the network has the ability to recover all of its neighbors;
b. Each node in the network can broadcast some essential messages to its neighbors with high reliability;
c. Each node in the network possesses a unique ID that can be distinguished from others.
d. The system is equipped with some monitor mechanisms or intrusion detection units either in the network layer or the application layer so that one node can observe the behavior of its one-hop neighbors.

A. Network Model of our Trusted AODV:



The above Figure is the flowchart of TAODV which will explain the performance of our Trusted AODV. In this work the first one involved in our flow is self-organized key management. This is included in our Trusted AODV is because through full self organization[10] security does not rely on any trusted authority or fixed server. A self-organized key management mechanism, such as threshold secret share solutions can cooperate with TAODV. These solutions provide secure ways to issue public key certificates which can be used for the generation and verification of digital signatures during the initialization of the TAODV or a newly joined node. In these cases , certificates are issued corporately by several nodes, which is consistent with the ways of updating trust relationships in the TAODV. Furthermore , the TAODV and the self-organized key management scheme can benefit from each other. The selection of trusted certificate issuers in this can refer to the trust information among nodes; and the digital signature extension is a good supplement to perform trusted routing operations.

B. Trust Representation:

Here a node's opinion about other nodes is modified to a 3-dimensional metric as follows

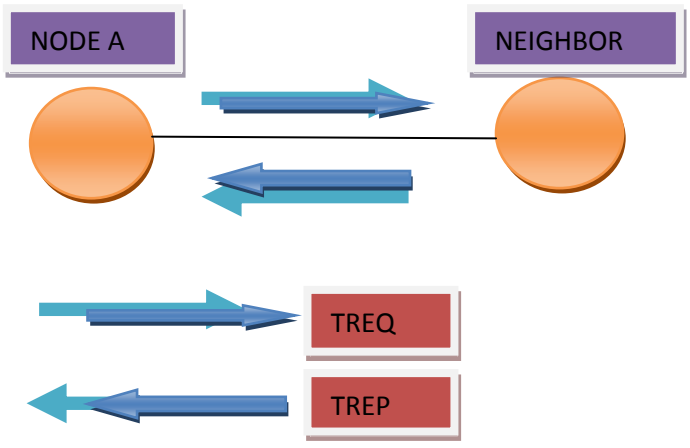
Let $W^{AB} = (b^{AB}, d^{AB}, u^{AB})$ denote any node A's opinion about any node B's trustworthiness in a MANET , where the first, second and third component correspond to belief, disbelief and uncertainty, respectively

C.Trust Combination:

In our trust model, a node will collect all its neighbors' opinions about another node and combine them together using combination operations. In this way , the node can make a relatively objective judgment about another node's trustworthiness even in case several nodes are lying.

D.Trust Recommendation:

In TAODV we devise an efficient Trust Recommendation mechanism. There are two types of messages used in the recommendation procedures: Trust Request Message (TREQ) , and Trust Reply Message (TREP). When a node A wants to know another node B's latest trustworthiness , it will broadcast an TREQ message to its neighbors. If one of A's neighbors receives the TREQ message then the neighbor will reply with an TREP message.



E.Trust Judgment:

Some trust judging rules we have described here for the node to perform corresponding operation according to the values in its opinion about another node. Here 0.5 is the threshold value

1. If belief of opinion of W^{AB} >0.5 , A will trust B and continue to perform routing behaviors or begin to transmit data packets to B.
2. If disbelief of opinion of W^{AB}>0.5 , A will not trust B and will not perform routing. Accordingly the route entry for B in A's route table will be disabled after an expire time.
3. If uncertainty of opinion of W^{AB}>0.5 , A will request and verify B's digital signature.
4. If node B has no route entry in node A's route table , A's opinion about B is initialized as (0,0,1)

F.Trust Updating:

a. Each time a positive event occurs from node A to node B, B's number of successful events in A's routing table will be increased by 1.
b. Each time a negative event occurs from node A to node B, B's number of failed events in A's routing table will be increased by 1.
c. Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using the evidence space to the opinion space.
d. Each time when the new opinion has been obtained through combination, the corresponding number of successful or failed events will be mapped back to the initial value (0,0,1).
e. The positive events include successful data or routing packets forwarding, keeping message integrity, and passing cryptographic verification, and so on.

IV.Intrusion Detection (Security Protocol) Algorithm

An intrusion can be defined as a subversion of security to gain access to a system. This intrusion can use multiple access methods and can span long periods of time. The aim of an intrusion detection system is to detect attacks against computer systems and networks. The algorithm can be summarized from the Fig II.A.1 as follows

1. During route discovery, a source node sends RRl packets to its neighboring nodes. In these packets along w the regular information , the node also sends its secu related information, such as key information.
2. Once an RREQ packet is received by an intermedi node, the node places the link trustworthiness and QoS information in the RREQ packet and forwards it to its next hop. This process is repeated until it reaches the final destination.
3. At the destination, the node waits for affixed number of RREQs before it makes a decision. Or else, a particular time can be set for which the destination or intermediate node needs to wait before making a routing de3cision. Once the various RREQs are received, the destination node compares the various TQI index values and selects the index with the least cost. It then unicasts the RREP back to the source node. When the source node receives the RREP, it starts data communication by using the route.
4. Once the route is established, the intermediate node monitors the link status of the next hops in the active routes. Those that do not meet the performance and trustworthiness requirements will be eliminated from the route.
5. When a link breakage in an active route is detected, a route error (RERR) packet is used to indicate the other nodes that the loss of that link has occurred.

V.SIMULATION RESULTS

Hardware used:

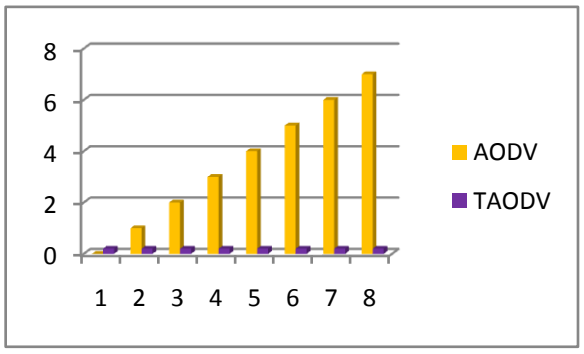
Processor	: Pentium III
Processor speed	: 1.5 GHZ
Memory (RAM)	: 256MB
Hard disk	: 40GB

Software used:

Operating System	: Linux 8.0(fedora 8.0)
Language	: TCL Scripting
Software	: ns2.34

Table 1

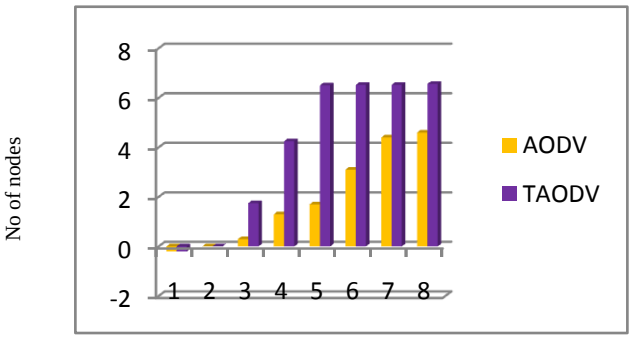
Parameters	Values
Examined protocol	AODV, TAODV
Traffic type	UDP
Transmission range	100m
Packet size	1024 bytes
Data rate	100 kb/s
Pause time	10 s
Minimum speed	1 m/s
Simulation time	900 s



FigV.1: Packet Drop vs. No of Nodes

The graph shows that as the percentage of malicious nodes participating in the mobile ad hoc network increase, the packet drop decreases because these malicious nodes tend to drop packets as they are forwarded. The outcome of dropping

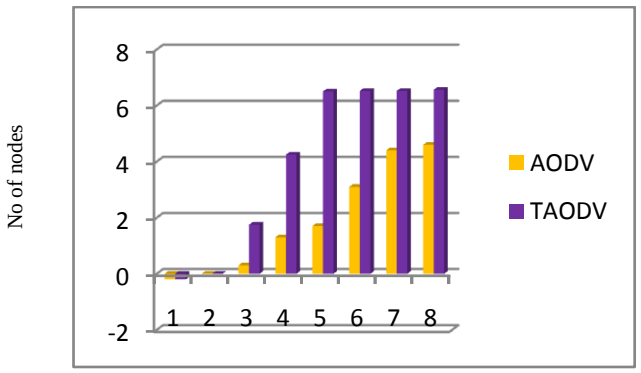
packets affects the normal AODV protocol during the full life of the network, but in case of TAODV, it is just affected partially as by time the malicious nodes will be identified and eliminated. The increase of packet drop of the network in the case of using TAODV is attributed to that each node uses opinion about other nodes' trust from the routing table.



Throughput

FigV.2:Throughput vs. No of Nodes

The graph shows that as the percentage of malicious nodes participating in the mobile ad hoc network increase, the throughput decreases because these malicious nodes tend to drop packets as they are forwarded. The outcome of dropping packets affects the normal AODV protocol during the full life of the network, but in case of TAODV, it is just affected partially as by time the malicious node will be identified and eliminated. The increase of throughput of the network in the case of using TAODV is attributed to that each node uses its local table of other nodes' trust values in the selection of the next-hop node for establishing the data route.



Packet Delivery Ratio

FigV.3: Packet Delivery Ratio vs. No of Nodes

From the graph, it is clear that when there are no selfish nodes in the mobile ad hoc network, both normal AODV and trusted AODV have almost identical number of packets reaching their destinations. The trusted AODV protocol is as normal AODV efficient as in delivering the packets and discovering routes to any destination. With increasing the percentage of selfish nodes in the network, there is a remarkable fall in normal AODV's number of packets reached since the network becomes more fragile but in the case of TAODV it is only partially affected by time.

VI. CONCLUSION

Secure Routing is one of the most basic and important tasks in MANETs. This paper reviewed various secure routing protocols based on AODV and from the comparative studies it is quite clear that these protocols are vulnerable to various routing attacks. Hence, we proposed the implementation of Trusted Ad-hoc On Demand Vector (TAODV) protocols.

The performance of Trusted Ad-hoc On Demand Vector (TAODV) protocols has been analyzed by including the source route accumulation feature. Since MANET's has limited range due to low transmission power the transfer of data packet from onenode to other implied threats due to malicious nodes.Also since it uses random wave generation we considered designing a solution for malicious attacks.

Based on the trust model, we design trusted routing protocols using intrusion detection system (secure protocol). We extend the routing table and the routing messages of AODV with trust information which can be updated directly through monitoring in the neighborhood. The more the positive events are collected, the higher the belief value in the opinion will be. Besides, a trust recommendation protocol was combined and the recommended opinions are gathered to have a judgment on each element of the new opinion. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedures can be guaranteed as well.

We also have included the synchronization of the trust level settings on different nodes when multiple paths cross with each other. By adapting cryptographic schemes (encryption and decryption) we collected the recommendations from different nodes to obtain the opinions.

Hence our comparative analysis of TAODV with that of AODV showed that the performance of TAODV is better than the previous AODV protocols and also it detected and eliminated the malicious nodes,by using trust relationship with the neighboring nodes.

VII. REFERENCES

[1]. DalipKamboj and Pankaj Kumar Sehgal, "A Comparative Study of various Secure Routing Protocols based on AODV", International Journal of Advanced Computer Science and Applications,Vol. 2, No. 7, 2011, pp 80-85.

[2]. G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, pp 815-819.

[3]. MohdAnuarJaafar 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 ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443.

[4]. R. S. Mangrulkar, Pallavi V Chavan and S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT", International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010, pp 36-39.

[5]. Shilpa S G, Mrs. N.R. Sunitha, B.B. Amberker, "A Trust Model for Secure and QoS Routing in MANETS", INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711) VOL.1 NO.5MAY 2011, pp 22-31.

[6]. Suchita Gupta, AshishChourey, " PERFORMANCE EVALUATION OF AODV PROTOCOL UNDER PACKET DROP ATTACKS IN MANET", International Journal of Research in Computer Science eISSN 2249-8265 Volume 2 Issue 1 (2011) pp. 21-2.

[7]. A.MenakaPushpa M.E., "Trust Based Secure Routing in AODV Routing Protocol", IEEE2009.

[8]. Songbai Lu1, Longxuan Li and Kwok-Yan Lam, LingyanJia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", IEEE 2009 International Conference on Computational Intelligence and Security, pp 421-425.

[9]. Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009.

[10]. S.Capkun, L.Buttyan, and J.-P. Hubaux. Self-organized public key management for mobile ad hoc networks. In Proceedings of ACM Workshop on Wireless Security (WiSe '02) , Atlanta , USA, September 2002.