IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

Secured & impregnable Cluster based Efficient routing Scheme for MANET

Prakash Patel
prakashpatel55@gmail.com
Prof. Anil Panwar

Abstract — ***an ad-hoc network is a multi-hop wireless network where all lumps cooperatively uphold network connectivity deprived of a consolidated substructure. If there is an amendment in node locations dynamically, it is called a mobile ad-hoc network (MANET). Meanwhile the network topology alterations frequently, effectual adaptive steering protocols such as AODV, DSR are used. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission. In this paper we proposed a cluster based efficient secure AODV routing protocol. Our proposed routing algorithm will provide a better level of security and performance than existing works. The results parameters will show in terms of improvement of the network performance, in terms of overhead, and end to end delay to the secure AODV routing protocol.***

Keywords —**MANET, Efficient Routing, AODV, Network Security, Network Lifetime, Cluster Network, Wireless Network.**

I. INTRODUCTION

MANET is a highly challenged network environment due to its special characteristics such as decentralization, dynamic topology and neighbor based routing. MANET can be applied to situations where an infrastructure is unavailable or deploying one is not cost effective. Such situations include disaster recovery, military field's communications, or some other crisis management services. The topology of MANET may change uncertainly and rapidly due to high mobility of the independent mobile nodes. Because of network decentralization, each node in MANET would act as a "router" to discover a routing path or to forward the data packets. Unlike wired networks, the functional design of MANET must take into account many factors such as wireless link quality, power limitation, and multi-user interference and so on.

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following types: External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. In this paper we proposed an efficient secureAODV routing protocol. The objective of proposed SAODV routing protocol is to secure routing packets of AODV protocol in MANET. The AODV protocol's routing have been improved to secure AODV.

To reduce the energy consumption in mobile devices, there have been efforts in physical and data link layers as well as in the network layer related to the routing protocol. The physical layer can save energy by adapting transmission power according to the distance between nodes. At the data link layer, energy conservation can be achieved by sleep mode operation.

The purpose of power-aware routing protocols is to maximize the network lifetime. The network lifetime is defined as the time when a node runs out of its own battery power for the first time [1]. If a node stops its operation, it can result in network partitioning and interrupt communication. The power-aware routing protocols should consider energy consumption from the viewpoints of both the network and the node levels. From the network point of view, the best route is one that minimizes the total transmission power. On the other hand, from the viewpoint of a node, it is one that avoids the nodes with lower power. It is difficult to achieve these two objectives simultaneously. Minimizing the total energy consumption tends to favour min-hop routes. However, if the min-hop routes repeatedly include the same node, the node will exhaust its energy much earlier than the other nodes

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

and the network lifetime will decrease. In a wide sense, ad hoc routing algorithms can be classified into the pro-active and the on-demand routing algorithms. The on-demand routing algorithms [2][3] start to find out the suitable route when a route is requested while the pro-active scheme [4] exchanges routing information periodically and generates the routing table in advance. Paper [5] shows that the on-demand routing outperforms the pro-active in terms of both delivery ratio and routing overhead. This is because it is difficult to find out the proper exchange rate of control packets, which depends on the mobility. The pro-active scheme has the possibility that some routing information exchanged is useless. That is, a slow exchange rate can make the routing information stale, and a fast rate results in excessive routing overhead. Therefore, it is a natural choice to design a power-aware routing protocol based on the on-demand scheme.

Conventional routing protocols [2] [3] [4] for ad hoc networks select the routes under the metric of the minimum hop count. Such min-hop routing protocols can use energy unevenly among the nodes and thus it can cause some nodes to spend their whole energy earlier as indicated in Section 1. As shown in the following examples, the feature of a power-aware routing protocol mainly relies on its metric. Candidates for the power-aware routing metric are considered in [7], and the performance of the power-aware routing protocols with different metrics is evaluated in [6].

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following types: External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy.

On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. There are many researches already done on the field of security related to mobile devices in mobile Adhoc Networks including [8] [9] [10] [11] [12] [13].

II. Background Techniques AODV

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad-hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

III. Working of AODV

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded. However, AODV operation does require certain messages (e.g., RREQ) to be disseminated widely, perhaps throughout the ad hoc network. The range of dissemination of such RREQs is indicated by the TTL in the IP header. Fragmentation is typically not required. As long as the endpoints of a communication connection

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

have valid routes to each other, AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request. Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations (possibly subnets) which are no longer reachable by way of the broken link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbours that are likely to use it as a next hop towards each destination. The information in the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to a node in a precursor list. If the RREP has a nonzero prefix length, then the originator of the RREQ which solicited the RREP information is included among the precursors for the subnet route (not specifically for the particular destination).

A RREQ may also be received for a multicast IP address. In this document, full processing for such messages is not specified. For example, the originator of such a RREQ for a multicast IP address may have to follow special rules. However, it is important to enable correct multicast operation by intermediate nodes that are not enabled as originating or destination nodes for IP multicast address, and likewise are not equipped for any special multicast protocol processing. For such multicast-unaware nodes, processing for a multicast IP address as a destination IP address MUST be carried out in the same way as for any other destination IP address. AODV is a routing protocol, and it deals with route table management. Route table information must be kept even for short-lived routes, such as are created to temporarily store reverse paths towards nodes originating RREQs.

AODV uses the following fields with each route table entry:

- ***Destination IP Address***
- ***Destination Sequence Number***
- ***Valid Destination Sequence Number flag***
- O***ther state and routing flags (e.g., valid, invalid, repairable, being repaired)***
  - → ***Network Interface***
  - → ***Hop Count (number of hops needed to reach destination)***
    - ***Next Hop***
    - ***List of Precursors***
    - ***Lifetime (expiration or deletion time of the route)***

Managing the sequence number is crucial to avoiding routing loops, even when links break and a node is no longer reachable to supply its own information about its sequence number. A destination becomes unreachable when a link breaks or is deactivated.

When these conditions occur, the route is invalidated by operations involving the sequence number and marking the route table entry state as invalid.

IV. CLUSTER BASED EFFICIENT ROUTING SCHEME

Average residual battery power Estimation

Basically the nodes use their residual battery power for the rebroadcast time of RREQ packets. If the time is determined only by the nodes' absolute residual battery power, then the retransmission time will increase as time passes by. Therefore, the relative measure should be used.

As a relative measure, we used the average residual battery power of the entire network. The exact value of this average power can be acquired by periodic control packets, but using periodic control packets isn't an on-demand method and it also consumes more energy. To estimate the average energy, our proposed algorithm uses only RREQ packets that

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

are already used in on-demand routing. For this end, *R* and *N* fields are added to the packet header, where *R* is the average residual battery power of the nodes on the path and *N* is the number of hops that the RREQ packet has passed. The mechanism to obtain the estimated average value is as follows.

1. First, the source records its own battery power to the *R* field, and sets the *N* to 1, and broadcasts the RREQ packet.

2. Assume that a node *I* has received an RREQ packet, and the node *i*'s residual battery power is *Bi* and the R_{value} of the RREQ packet is $\overline{R}_{old}$. Then the average residual battery power, R_{new}, of new route that includes the node$_i$ is as following

$$\overline{R}_{new} = \frac{\overline{R}_{old} \times N + B_i}{N+1} \quad (1)$$

Before the node *I* rebroadcasts the packet, it updates *R* to R_{new} and increases the value of *N* by one. This step is not executed for duplicate RREQ packets.

3. Whenever a node *I* receives an RREQ packet, it calculate the average residual battery power of the network by the following equation.

$$\tilde{E}_{new} = (1-\alpha)\tilde{E}_{old} + \alpha\overline{R}_{old} \quad (2)$$

Where, α is the weighting factor of the moving average. Theα is set to 0.75 in our simulations.

The objective of proposed SAODV routing protocol is to secure routing packets of AODV protocol in MANET.
The AODV protocol's routing have been improved to secure AODV. The proposed SAODV have three components. These are Hash Chain, Digital Signature, and Protocol Enforcement Mechanism.
(1) Hash Chain used for securing the hop count
(2) Digital Signature for authentication
(3) Protocol Enforcement Mechanism using the enforcement this protocol will address of any nodes, which packets have been changes.

A. SAODV Hash Chains

Hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points, but by any node that receives one of those messages. Every time a node wants to send a RREQ or a RREP it generates a random number (seed). Select a Maximum Hop Count. Maximum Hop Count SHOULD be set to the TTL value in the IP header, and SHOULD never exceed its configuration parameter NET_DIAMETER.
The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Every time a node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count Hop Count times the Hash field, and checking that the resultant value is the same than the Top Hash. If the check fails, the node SHOULD drop the packet. Before rebroadcast a RREQ or forwarding a RREP, a node hashes one time the Hash field in the Signature Extension.
The function used to compute the hash is set in the Hash Function field. Since this field is signed, a forwarding node will only be able to use the same hash function that the originator of the routing message has selected. If a node cannot verify or forward a routing message because it does not support the hash function that has been used, then it drops the packet.

B. SAODV Signatures

When calculating signatures, Hop Count field is always zeroed, because it is a mutable field. In the case of the Signature for RREP field of the RREQ Double Signature Extension, what is signed is the future RREP message that nodes might send back in response to the RREQ. To construct this message it uses the values of the RREQ and the Prefix Size (the RREP field that is not derivable from the RREQ but not zeroed when computing the signature. In the case of RREPs, R and A flags are also zeroed. SAODV is not designed taking into account AODV multicast ('R' flag is used in multicast) and 'A' flag is mutable and, if an attacker alters it, it can only lead to some sort of denial of service. Every time a node generates a RREQ it decides if it should be signed with a Single Signature Extension or with a Double Signature Extension. All implementations MUST support RREQ Single Signature Extension, and SHOULD support RREQ Double Signature Extension. A node that generates a RREQ with the gratuitous RREP flag set SHOULD sign the RREQ with a Double Signature Extension. A node SHOULD never generate a RREQ without adding a Signature Extension. When a node receives a RREQ, first verify the signature before creating or updating a reverse route to that host. Only if the signature is verified, it will store the route. If the RREQ was received with a Double Signature Extension, then the node will also store the signature, the lifetime and the Destination IP address for the RREP in the route entry. If a node

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

receives a RREQ without a Signature Extension it SHOULD drop it. An intermediate node will reply a RREQ with a RREP only if fulfils the AODV requirements to do so, and the node has the corresponding signature and the old lifetime and old originator IP address to put into the 'Signature', 'Old Lifetime' and 'Old Originator IP address' fields of the RREP Double Signature Extension. Otherwise, it will rebroadcast the RREQ. When a RREQ is received by the destination itself, it will reply with a RREP only if fulfils the AODV requirements to do so. This RREP will be sent with a RREP Single Signature Extension. All implementations MUST support RREP Single Signature Extension, and SHOULD support RREP Double Signature Extension. A node SHOULD never generate a RREP without adding a Signature Extension. This also applies to gratuitous RREPs. When a node receives a RREP, first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will store the route with the signature and the lifetime and the originator IP address of the RREP. If a node receives a RREP without a Signature Extension it SHOULD drop it. Every node, generating or forwarding a RERR message, uses digital signatures to sign the whole message and any neighbour that receives verifies the signature.

C. the Proposed SAODV Algorithms to handle the routing packets:

Algorithm1: Receiving RREQ Packets from the originator

//

1. Start
2. Packet Classifier Packets
3. If (RREQ secure)
4. Packet extractor RREQ secure
5. Packets: Original RREQ + Hash Chin protection created in node + digital signature + protection Key.
6. Hop count tester hop count + max hop + top hash
7. Signature verification Protection key + digital signature
8. If (hop count tester and signature verification is matched)
9. Then update route
10. End if
11. If (node = destination)
12. Signature generate non mutable RREQ
13. Hash chain generate 0; packet Builder RREP + Hash Chain protection + digital signature + protection key
14. Sent RREP to lower layer 15. Else
16. Packet forward RREQ
17. End if

//

Algorithm 2: Broadcast RREQ packet

//

1. Start
2. Packet destination RREQ
3. Next hop = find the as packet destination
4. If (next hop= null)
5. Then
6. Packet forward RREQ
7. Else
8. Signature generator non table RREQ
9. Hash chain protect generator 0;
10. Packet builder RREQ + hash chain protection + digital signature + protection key of the node
11. Broadcast
12. End if

//

Algorithm 3: Receiving RREP packets

1. Start
2. Packet destination = extractor RREP
3. Packet origin= extractor RREP
*4. *//Route entry for find this node (destination) //**
5. If (route entry = null)
6. Addition route as routing success
7. Else
8. Routing not success
9. End if
10. If(node address= packet destination)
11. Generate RREP and receiving RREQ algorithm
12. Else
13. Forward packet in next node in the route
14. Forwarding route reply
15. End if
16. End if

//

Packet arrive to the system will be identified by the packet classifier to determine the type of packet. This protocol has four packet types. These are Route Request Secure (RREQ), Route Reply Secure (RREP), Route Error Secure (RERR) and Hello Packet. All packets except the hello packets will be extracted to identify component within the packets.

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

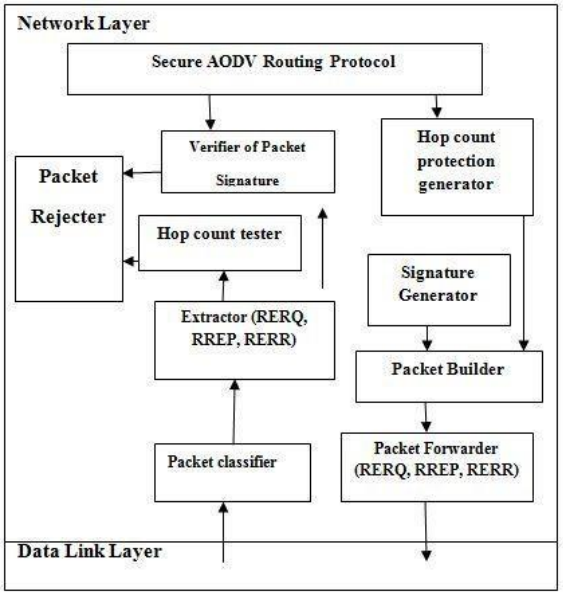

Fig 1: Architecture of Secure AODV routing protocol

This will be followed by the integrity evaluation and hop count verification of the extracted packets. Two modules; these are the packet signature verification and hop count tester will handle these task. Also at this point, the RERR Secure is executed from the hop count verification as this packet has no hop count, but integrity evaluation is still considered on this packet. Any alternation to the hop counts of RREQ Secure and RREP secure either by incrementing or decrementing the value will trigger the hop count tester to generate error notification and will reject the packet through packet rejecter. The violation of the packet integrity will also trigger error notification and will reject the packet reject too. If the evaluation and verification are succeeding, this protocol may update routing information to routing table. Before passing the packet, call hop count protection generator hash from, and then the packet builder warps the signature, hop count protection, and public key into secure packet and pass them to packet forwarder.

IV. SIMULATION RESULTS

A comparison of the delivery ratio among power-aware routing algorithms. We can see that the better power-aware routing algorithms also have a better delivery ratio. Our protocol showed the highest delivery ratio of about 95%, which is approximately 13% higher than that of the traditional routing.

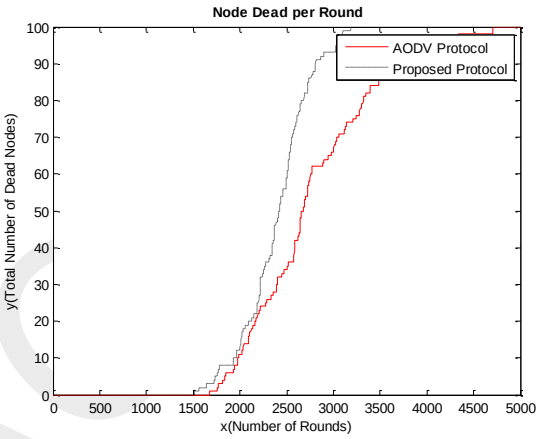

Figure. 2. Expiration sequence of node

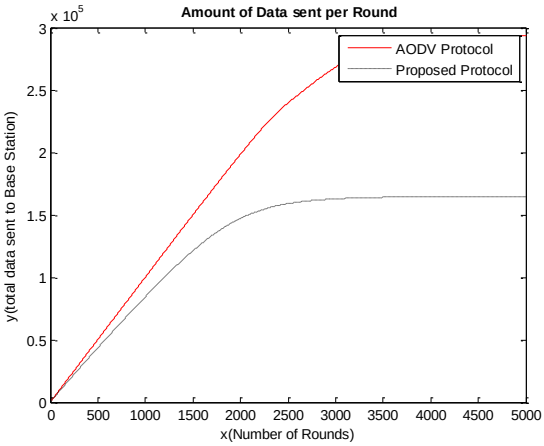

Figure. 3. Data packets Sent to base station

The reason why the delivery ratio is proportional to the performance of power-aware routing is because the nodes with less residual battery power are excluded from the route in power-aware routing algorithms. If the established route contains a node which has small residual battery power, the node will consume all its battery powered.

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

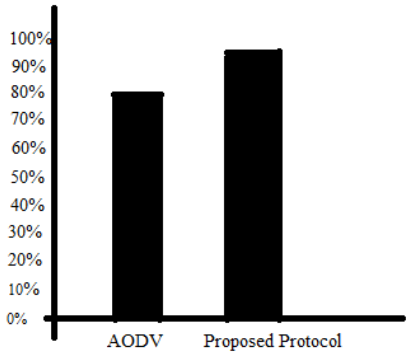

Figure 4. Delivery ratio in mobile environment

The reason why the delivery ratio is proportional to the performance of power-aware routing is because the nodes with less residual battery power are excluded from the route in power-aware routing algorithms. If the established route contains a node which has small residual battery power, the node will consume all its battery power. Then the route will break in the middle of data packet delivery and the remaining data packets will be lost. Therefore, the better the performance of power-aware routing, the higher the reliability of the route and the delivery ratio.

V. Conclusion

The proposed approach use the security mechanisms so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. Selects nodes that have relatively abundant battery energy. Since the rebroadcast time dynamically varies according to residual battery power, our protocol keeps a balance between min-hop routing and fair battery consumption. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of our protocol tested in simulation and their communication costs were measure using the MATLAB SDE, which was suitable for the present purpose. The evaluation metrics in this study were total number of node dead, overhead, and delay ratio and in both the cases our protocol show better performance.

VI. References

[1]. Q. Li, J. Aslam and D. Rus: Online Power-aware Routing in Wireless Ad-Hoc Networks. Proceedings of MOBICOM, July 2001.

[2]. D. Johnson, D. Maltz: Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers (1996) 154-181.

[3]. C. Perkins, E. Royer: Ad-hoc On-Demand Distance Vector Routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[4]. C. Perkins, P. Bhagwat: Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. Proceedings of ACM SIGCOMM, August 1994.

[5]. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu and J. Jetcheva: A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. Proceedings of MOBICOM, October 1998.

[6]. C. K. Toh: Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks. IEEE Communications Magazine, June 2001.

[7]. R. S. Mangrulkar "*Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT*" International Journal of Computer Applications (0975 – 8887)

[8]. 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.

[9]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati, "Routing Security in Wireless Ad Hoc Networks"

[10]. Mohammad O. Pervaiz, MihaelaCardei, and Jie Wu "Routing Security in Ad Hoc Wireless Networks"

[11]. Huaizhi Li, Zhenliu Chen, Xiangyang Qin, Chengdong Li, Hui Tan "Secure Routing in Wired Networks and Wireless Ad Hoc Networks"

[12]. Lidong Zhou and Zygmunt J. Haas, Cornell University "Securing Ad Hoc Networks"

[13]. Dr. Harsh Sadawarti and Anuj K. Gupta, Member, IAENG, "Secure Routing Techniques for MANETs" International Journal of Computer Theory and Engineering