International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Detection and Recovery of Intruder Node in Mobile Ad Hoc Networks

Narender Sharma[1], Mrs. Poonam Sehrawat[2]
[1]Narender Sharma
M.Tech. Student
Department of ComputerScience & Applications
Chaudhary Devi Lal University, Sirsa
narender_sbhardwaj@yahoo.co.in
[2]Mrs. Poonam Sehrawat
Assistant Professor
Department of ComputerScience & Applications
Chaudhary Devi Lal University, Sirsa
poonamsehrawat6@gmail.com

Abstract: *Protection from Intruders is very challenging and important security issue in Mobile Ad hoc networks. In this paper, a modified AODV algorithm has been proposed to identify and deactivate intruder nodes. The proposed algorithm based on existing AODV routing protocol. In this modified AODV algorithm does not use any cryptographic portion on the messages which will transmit. But, this proposed Modified AODV routing protocol protecting the network by detecting and deactivating the Intruder nodes. To prove the practical significance of the approach, this approach is implemented on NS2. Experimental evaluation shows the efficiency of proposed algorithm in terms of Throughput, Packet Delivery Ratio and End to end delay.*

Keywords: *Mobile ad hoc networks, Intruder Detection, routing misbehavior.*

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) [1] is a group of mobile nodes that cooperate and forward packets for each other. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which predeployed infrastructure support is not available. MANETs have some special characteristic features [3] such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low computation power etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks. MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior of any participating node(s). One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this paper, the attack known as Black Hole Attack [2] has been discussed on the widely used AODV (Ad hoc On-demand Distance Vector) routing protocol in MANETs. A new mechanism has been proposed to detect and defend the network against such attack which may be launched cooperatively by intruder nodes.

The rest of the paper is organized as follows. Section II describes related work in literature; Section III describes problem statement and gives the details of the proposed solution. Section IV presents the simulations and the performance analysis of the scheme. Section V concludes the paper with future scope of work**.**

II. RELATED WORK

In MANETs the Denial of Service, intruders attack is very active and therefore it is gaining the attention of the researchers. The main focus of the research is to either secure the existing protocol or to develop a new secured routing protocol. Awerbuch et al. [6] developed a secure new on-demand routing protocol. It includes link weights which are considered during route discovery. The weights are calculated from the packet delivery fraction of each link. A link not delivering a fraction of packets above a certain threshold is considered malicious and therefore the link weight is increased such that the link is chosen with smaller probability in the next route discovery phase. The approach detects a black hole as soon as the impact occurs, not when the black hole is constructed. In [7] a secure routing protocol based on the Dynamic Source Routing (DSR) protocol is presented. The authenticity of Route Requests is verified using message authentication codes (MAC). Furthermore, the authors present three techniques for authenticating data in Route Requests and Route Replies. A broadcast authentication protocol for authenticating routing messages called TESLA[8, 9] uses digital signatures. Additionally, the authors propose per-hop hashing to verify that no node present in the node list of the Route Request is removed by an attacker. Abdul-Rahman et al [10] have proposed a *distributed trust model* - a decentralized approach to trust management that uses a recommendation protocol to exchange trust-related information. The model assumes that relationships are unidirectional and exist between and two entities (nodes). The entities make judgments about the quality of a recommendation of trust, based on their policies, i.e., they have values for trust relationships. The recommendation protocol works by requesting a trust value in a trust target with respect to a particular classification. After getting an answer, an evaluation function is used to obtain an overall trust value in the target node. The protocol also allows recommendation refreshing and revocation, and is suited for establishing trust relationships that are less formal and temporary in nature. Asokan et al[11] have introduced several password-based key exchange methods to set up a secure session among a group of nodes without any support infrastructure. In this scheme, only those nodes that know an initial password are able to obtain the session key. A weak password is sent to the group members. Each member then contributes to generation of part of the key and signs this data by using the weak password. Finally, to establish a secure session key, a secure channel is derived without any central trust authority or support infrastructure. Stajano et al [12] have introduced the *resurrecting duckling* security protocol to establish trust in ad hoc networks. The protocol is particularly suited for devices without display and for embedded devices that are too weak for public key operations. The fundamental authentication problem is solved by a secure transient association between two devices establishing a master-slave relationship. It is secure in the sense that the master and the slave share a common secret. The protocol is transient because the master at any point of time can terminate the association. Repantis et al[13] have proposed a decentralized trust management middleware for ad hoc, peer-to-peer networks based on *reputation* of nodes. The reputation information of each peer is stored in its neighborhood and piggybacked on its replies. Patwardhan et al[14] have proposed a trust-based data management scheme in which mobile nodes access distributed information, storage and sensory resources available in pervasive computing environment. The authors have taken a holistic approach that considers data, trust, security, and privacy and utilizes a collaborative mechanism that provides trustworthy data management platform in an ad hoc network.

III. PROPOSED WORK

Intruders attack is a severe denial-of-service attack routing protocol threat, accomplished by dropping packets, which can be easily employed against routing in MANETs, and has the effect of making the destination node unreachable or downgrade communications in the network. The black holes are invisible and can only be detected by monitoring lost traffic. The emergence of new applications of MANETs necessitates the need for strong privacy protection and security mechanisms. In the proposed scheme intruder nodes can perform many attacks by taking advantage of the loopholes in the protocol and thus can cause drop in packets [4]. A new scheme has been proposed which takes care of the intruder attack [2] which exhibits packet forwarding misbehavior. In a intruder attack malicious node replies to every route request by falsely claiming that it has a fresh enough routes to the destination. In this way all the traffic of the network are redirected to that intruder node which then dumps them all. The new scheme takes care of this critical situation by detecting the intruder node and then selecting a new path for smooth transfer of packets.

Proposed plan has been incorporated on AODV protocol, but its principal will be applicable to other routing protocol as well. In this scheme the famous AODV routing protocol is modified, a new field, next_hop, in the routing messages has been added, so that a node can correlate the overheard packets accordingly. In the proposed plan three important sections of algorithms are implemented. In algorithm

Section 1 describes modified route request procedure, Section 2 discusses route reply procedure and Section 3 discusses the packet forwarding procedure respectively. Each node in order to participate in any network activity, says Route Request (RREQ), has to announce it's token as described in Algorithm Section 1. If the node bit Node_type is "1" indicating intruder node, protocol does not allow the node to participate in any network activity. Otherwise, the Node_type bit is "0" indicating Non intruder node, which confers it the freedom to participate in all network activities.

Algorithm section 1: Working of RREQ packet

1: Set Node_type "0" or "1"
Node_type = "0" means non intruder node
Node_type = "1" means intruder node
2: Broadcast RREQ packet (p) by source node
3: if node Node_type = "0" then broadcast RREQ to this node
If Node_type = "1" then deactivate this node and don't broadcast RREQ
4: repeat steps 2 and 3 until it reaches to Goal

Algorithm Section2: Working of RREP packet

1: Destination node rebroadcast the RREP packet like the RREQ
2: All the possible routes will be searched by RREP
3: If any node is out of signal range or dead from the network after getting RREQ then available route will be selected by the RREP broadcasting. No need to rebroadcast RREQ and then re- reply for select the routing path
4: repeat steps 2 and 3 until it reaches to source node
5: Source node will select the path for data transmissions based on shortest path

Algorithm Section 3: Data Packet Transmission

1: Set counter at every node
2: After receiving an overhearing message, node will compare the data packet, send by it, with the counter value.
3: If any node does not receives overhearing message than successor node is declared as malicious node by setting its htype= "1".
4: After detecting intruder node *an error message will be generate by the node and send it to the source node. Source node will declare it as* intruder node *by making its Node_type= "1" in the routing table and the present route will be deactivated.*
5: Source node select alternate route for data transmission.

IV. SIMULATION MODEL

The performance of the proposed modified AODV routing protocol performed by using the network simulator NS-2.34 using the operating system Ubuntu 10.04.

To Analysis the performance of proposed Routing Algorithm some measures are used like Throughput, Packet Delivery Ratio and End to end delay has been used. During the all scenarios of simulation the number of intruder nodes is 10%. Different speeds and different number of nodes are taken for analysis.

Table 1: Simulation parameters

Routing Protocol	AODV and Proposed Modified AODV
Communication Type	CBR
Number of Nodes	10, 20, 50
Maximum mobility speed of nodes	0,2,4,6,8,10 m/sec
Simulation Area	750 m x 750m, (1000m x 1000 m for 50 nodes only)
Simulation Time	250 sec
Packet Size	512 bytes
Number of Intruder nodes	1, 2, 5

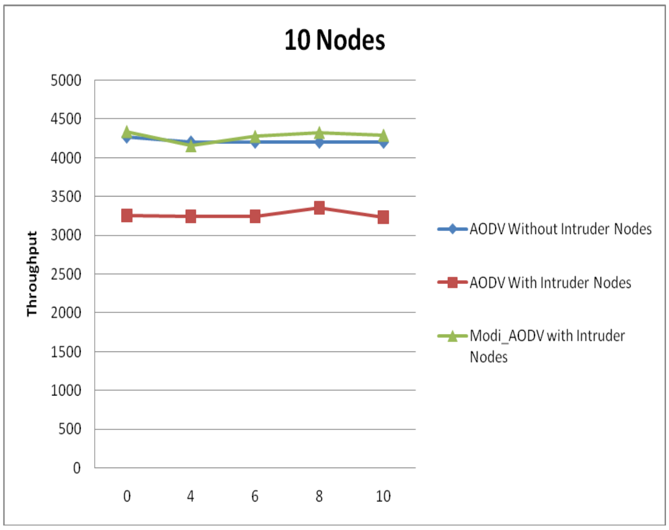

Figure 1: Throughput vs. speed

Figure (1) describes throughput in kbps. While AODV simulate exclusive of intruder attack throughput among 4203kbps to 4268.38 kbps in every movement speed situation except while AODV simulate through intruder attack throughput drop downwards and arrive at approximately 3231 kbps to 3354.02 kbps. Other than while Modi_AODV simulate among intruder attack throughput once more approximately arrive at similar to AODV except is not capable to obtain 4153.86 kbps to 4340.24 kbps.

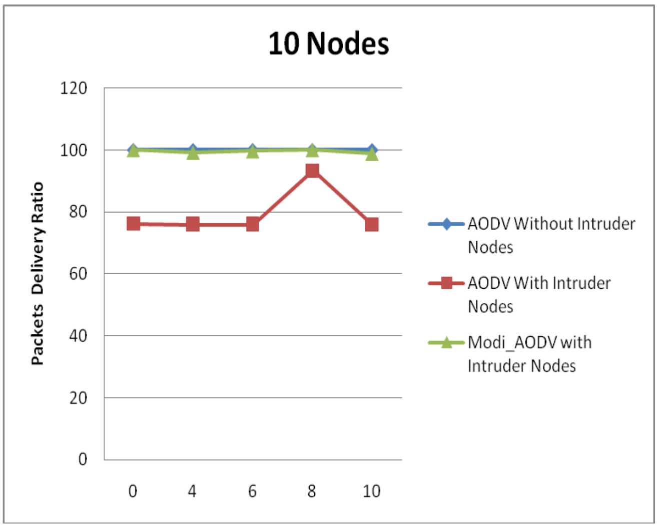

Figure 2: Packet Delivery Ratio Vs. speed

Figure (2) describes the PDR in %age. While AODV simulate exclusive of intruder attack PDR around 100% in all progress speed situation except while AODV simulate among intruder attack PDR fall downwards and achieve approximately 76% to 80.33%. However while Modi_AODV simulates with intruder attack PDR once more approximately arrive at similar to AODV and it obtains 98.8% to 99.98% accurateness.

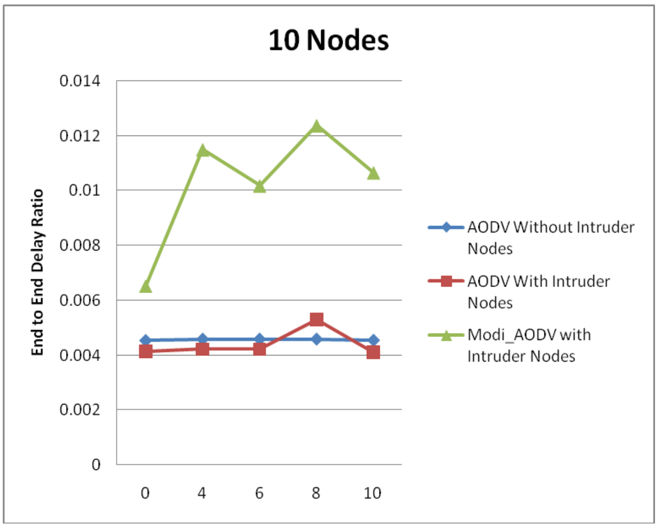

Figure 3: End to End Delay Ratio Vs. speed

Figure (3) describes End to End Delay Ratio in Seconds. While AODV simulates exclusive of intruder attack End to End Delay Ratio comes among "0.00454 Seconds and 0.00459 Seconds" in every one movement speed scenarios except while AODV simulates with intruder attack End to End Delay Ratio reach approximately 0.00411 Sec. to 0.00531 Sec. Except while Modi_AODV simulates through intruder attacks, then End to End Delay Ratio is elevated and it reaches approximately 0.00652 Sec. to 0.01238 Sec.

In the following figures the throughput, PDR and End to end delay ration is compared during intruder attack in existing AODV and in proposed modified AODV using 20 Nodes

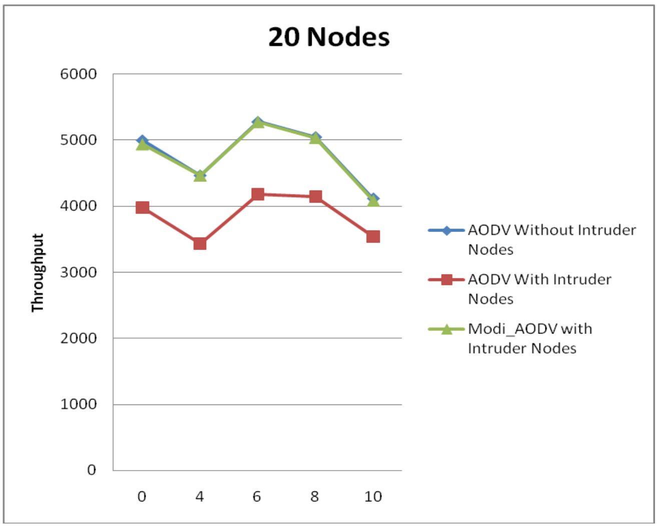

Figure 4: Throughput vs. speed

Figure 4 shows that the in existing AODV throughput is reducing around 500-1000 kb but in the case of proposed modified AODV throughput is almost same during the intruder attack. It shows that proposed Modified AODV is giving efficient results. Figure 5 shows the PDR is reducing around 10% to 30% in existing AODV while in the case of proposed modified AODV PDR is almost same during intruder attack

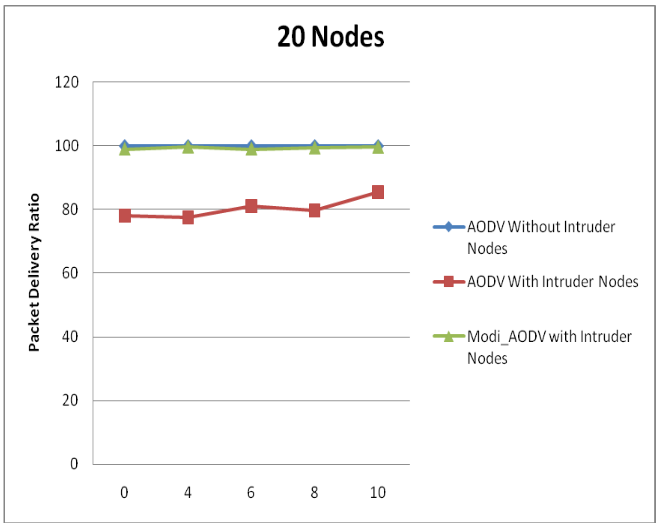

Figure 5: Packet Delivery Ratio Vs. speed

Figure (5) describes the Packet Delivery Ratio of AODV in the existence of intruder nodes, exclusive of intruder nodes and Modi_AODV. The Packet Delivery Ratio of AODV in the existence of intruder nodes is extremely less which is 77.43% to 85.35% in contrast of AODV exclusive of intruder nodes and Modi_AODV by way of intruder nodes that is 99.02% to 100%. The consequence of AODV exclusive of intruder nodes and Modi_AODV among intruder nodes is approximately similar which proves that Modi_AODV effectively detects and deactivates the contribution of intruder nodes from AODV.

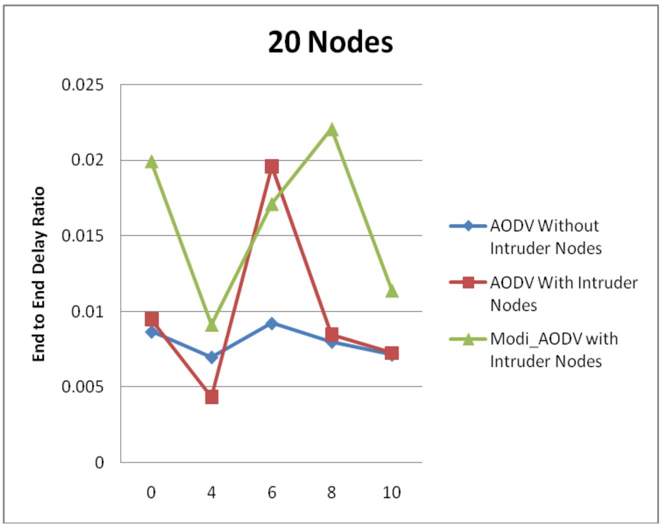

Figure 6: End to end delay ratio vs. speed

The figure 6 shows that the End to end delay is high in proposed modified AODV during intruder attack. The main reasons behind this perform is because of the dual role of intermediate nodes in the MANET. Every node is acting as a monitor as well as data transmitter so end to end delay is high. Moreover more calculations are needed at times of recovery and this may be cause of spikes.

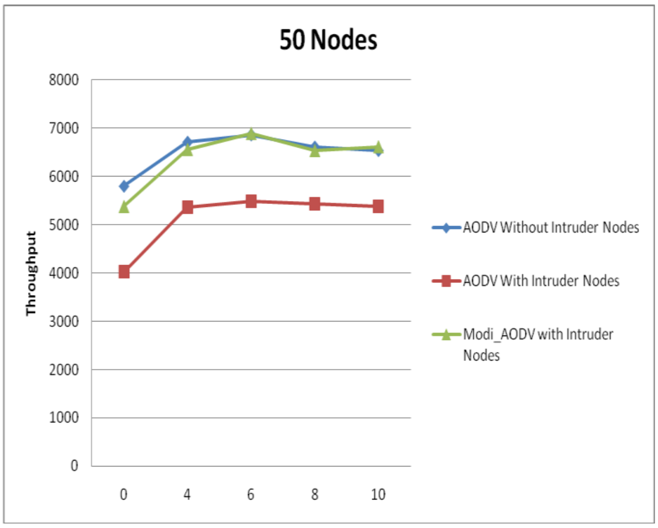

Figure 7: Throughput vs. speed

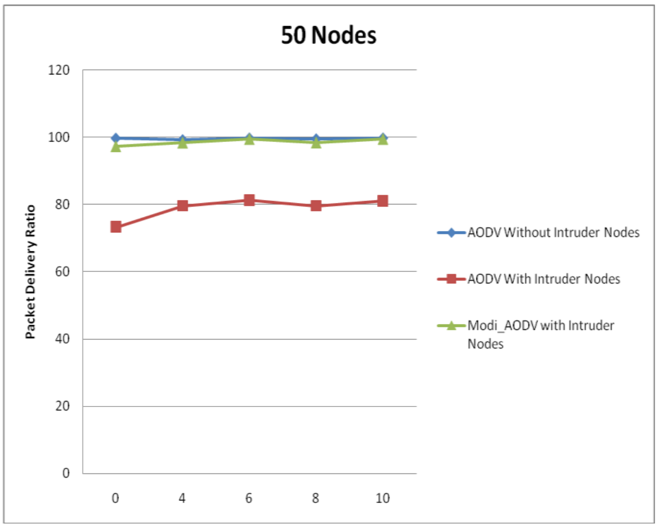

Figure 8: Packet Delivery Ratio Vs. speed

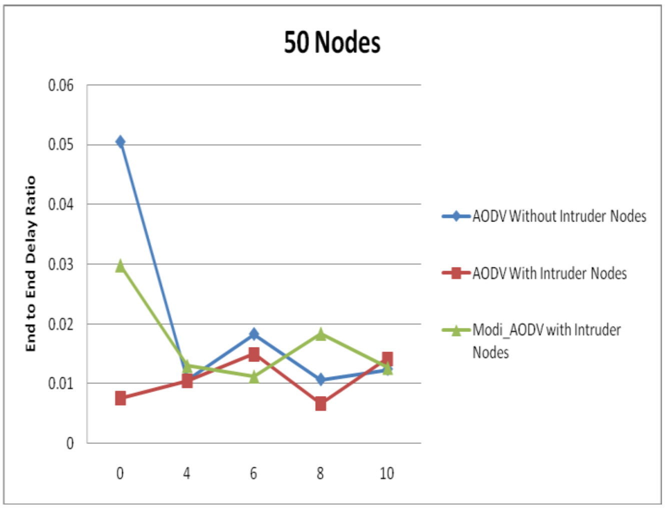

Figure 9: End to end delay ratio vs. speed

Figure 7-9 are represent a denser medium with 50 nodes. It shows that throughput in existing AODV throughput is reducing around 2500-3000 kb but in the case of proposed modified AODV throughput is almost same during the intruder attack. PDR is reducing around 40% to 50% in existing AODV while in the case of proposed modified it almost touches the original mark. End to end delay is performing much better in denser medium. The reason is that more nodes are available for recovery process. So lesser delay exists.

V. CONCLUSION AND FUTURE WORK

Introduced a novel secure routing protocol, termed as **Modi_AODV.** The proposed protocol is based upon hop count method from sender to target node. The scheme has been illustrated for AODV protocol and could easily be adopted for other on-demand routing protocols for providing stability, integrity and nonrepudiation. The proposed algorithm has been evaluated with different network parameters under a simulated environment. This is the first reported work for securing Ad hoc networks using hop count technique and selected route is compared with the longest alternative route to target which is second hop node.

REFERENCES

Vijay Kumar, Ashwani Kush, "*Proposed New Mechanism to Detect and Defend the Malicious Attackers in AODV*", ACSIJ Advances in Computer Science: an International Journal, Volume 2, 2013 - May 2013 Issue, No. 201, (pg 1-6), ISSN : 2322-5157(Iran).

Vijay Kumar, Rakesh Sharma, Ashwani Kush "*EFFECT OF MALICIOUS NODES ON AODV IN MOBILE AD HOC NETWORKS*", International Journal of Computer Science and Management Research ISSN 2278-733X, Vol. 1 Issue 3 October 2012.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, issue 3, Nov 2007, pp 338–346.

Shree Om, Mohammad Talib , " Using Merkle Tree to Mitigate Cooperative Black-hole Attack in Wireless Mesh Networks" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 5, 2011

C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000, http://www.ietf.org/internal-drafts/draft-ietf-manetaodv-05.txt

B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the 3rd ACM Workshop on Wireless Security, 2002.

Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and Secure Source Authentication for Multicast," In Network and Distributed System Security Symposium, pp. 35–46, February 2001.

J. T. A. Perrig, R. Canetti and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," In IEEE Symposium on Security and Privacy, pp. 56–73, May 2000.

A. Abdul-Rahman and S. Hailes, "A distributed trust model", in *Proceedings of the New Security Paradigms Workshop*, pp. 48-60, Langdale, Cumbria, United Kingdom, 1997.

N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks", *Computer Communications*, vol 23, no 17, pp. 1627-1637, 2000.

F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ad hoc wireless networks", in *Proceedings of the 7th International Workshop on Security Protocols*, LNCS 1796, Springer- Verlag, pp. 172-194, 1999.

T. Repantis and V. Kalgeraki, "Decnetralized trust management for ad hoc peer-to-peer networks", in *Proceedings of the 4th International Workshop on Middleware for Pervasive and Ad-Hoc Computing(IMPAC 2006)*, p. 6, Melbourne, Australia, April 2006.

A. Patwardhan, F. Perich, A. Joshi, T. Finin, and Y. Yesha, "Querying in packs: trustworthy data management in ad hoc networks", *International Journal of Wireless Information Networks*, vol 13, no 4, october 2006.

A.Kush, S.Taneja, Divya, "Encryption Scheme for Secure Routing in Ad Hoc Networks" in International Journal of Advancements in Technology http://ijict.org/ ISSN 0976-4860, Vol 2, No 1 (January 2011) pp22-29.