ISSN:0975-9646

Security Model to Detect and Avoid Wormhole Attack Using AODV Protocol

Gulzar Ahmad Wani [1], Dr. Sanjay Jamwal[2]

[1,2] *Department of Computer Science,*
Baba Ghulam Shah Badshah University, Rajouri, J&K, India

***Abstract*— The current demand of MANET is its security and robustness. MANET's operational performance also depends on security. An attacker can easily attack on MANET because of its open nature and bandwidth constraint. Most of research have been done on the MANET security. Wormhole attack is most severe threat to security of MANET. In which two far-away malicious nodes are linked to each other with high speed link called wormhole tunnel. Most of previous research work done on detection and prevention of wormhole attacks uses packet leashes, extra hardware (GPS, Directional Antenna etc.) and few modifies the source code of routing protocols to improve security. In this paper, we propose a security model that will detect and avoid the wormhole attack in MANET using routing protocol i.e., AODV protocol.**

Proposed security model has three phases. In the first phase, detection of malicious node is done by using Bogus RREQ and in second phase normal AODV operation is performed for detection of shortest path from source to destination. In the third phase, once again detection of attacker is done by using delay metric if there is presences of wormhole attack then it repeats from phase one otherwise selects the shortest route to destination discovered in phase second.

***Keywords*— Wormhole attack, MANET, AODV, Malicious node, Routing Protocols, Security.**

I. INTRODUCTION

Ad-hoc network is the modern image of wireless network especially for mobile node. A mobile ad hoc network (MANET) is a collection of two or more nodes that are continuously self-configuring, self-organizing and these mobile devices are connected with each other without wires as shown in below Fig. 1. Ad hoc network supports more advanced applications, such as transportations, military, security, health, educations, disaster recuperation, search and rescue and battlefields are the true examples where Ad-hoc network are used [1].

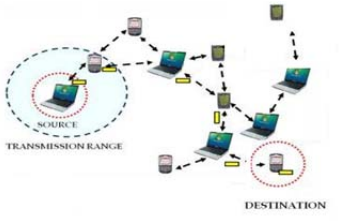

Fig. 1. Ad-hoc Network

Security in mobile ad-hoc network is the current significant issue of network. The Services of MANET like integrity and confidentiality of data is attained by facing and solving the security issue of MANET. The dynamic topology and open nature makes the wireless network (especially Mobile Ad-hoc Network) more vulnerable to security threats. The various loopholes that threaten the security of wireless network include wormhole, sink/black hole, MAC spoofing, Denial-of-Service attack , Network injection, worm hole, Man-in-the-middle attacks, Sybil attack and etc.

The wormhole attack [2] among all the attack is very severe threat to MANET and is very hard to detect. It is an attack that involves two malicious nodes and high speed link between them, the malicious node gets packet from one location and passes it to another malicious node which delivers it to destination node, and make source node to believe that it is the right route to send packet. The wormhole attack puts the malicious node in a high power to get the packet from its neighbours as compared to other legitimate nodes in the network. In Figure 2 M1 and M2 acts as malicious node that attracts the packets from their neighbour's and passes to other malicious node through tunnel.

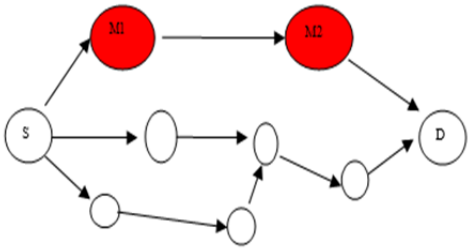

Fig. 2. Wormhole Attack

If the source node wants to send the packet to the destination and the destination node is not within the transmission range of source node then it uses multi-hop concept i.e., multi-hop routing protocols that routes the packets over multiple number of hops.

AODV Protocol is more efficient and robust amongst the reactive protocols. The AODV main goal is to reduce the routing overhead caused by the source node in DSR protocol. The AODV discovers route to network wide broadcasting. If a source node wants to send the packet to the destination. It broadcasts the RREQ to its neighbours. The neighbour node rebroadcasts the Route Request (RREQ) again if it does not have a valid route to destination to it is itself not a destination.

TABLE I
COMPARISON AMONG VARIOUS TECHNIQUES OF DETECTION AND AVOIDANCE TECHNIQUES

Methods	Description	Merits	Demerits
Geographical leashes [3].	Neighbour validation: Limit the packet travelling distance by using loose clock synchronization and location information.	Useful when tight Clock synchronization is not required	Use of hardware device like GPS. High network overhead, huge storage required.
Temporal Leashes [3].	Limit the propagation time of data packet using tight clock synchronization.	No extra hardware required.	Nodes must have accurate clock synchronization, huge storage required for authentication.
Directional Antennas [4].	Node transmit data through directional antennas. Connection is established when direction of antennas is matched	No location information and Synchronization of clock is needed. Efficient use of bandwidth and energy.	Infeasible to deploy the directional antennas in practice
Wormhole Avoidance Routing Protocol (WARP) [5].	Looks at Link-disjoint multi-path during path discovery and selects the one path from selection of paths for data transfer.	No clock synchronization and no hardware is needed.	Used to detect wormhole attack in both I / O bound mode.
Hop-Count based Technique [6].	Modification to AODV Route Discovery phase and makes selection of optimum path from a set of paths.	Efficient solution as compared to computational and hardware point of view.	Compromise in Hidden mode wormhole attack.

II. LITERATURE REVIEW

In wormhole attack, A lot of research has been done and various techniques has been proposed to detect and avoid the wormhole attack and are explained briefly in given below Table I

III. ANALYSIS OF WORMHOLE ATTACK AND AODV PROTOCOL

A. *Wormhole Attack.*

Wormhole is conjectural feature of topology that provides the short-cut through space. It is like a tunnel with two end points.

The wormhole attack [2] is the most serve attack in the network security which involves two malicious nodes and high speed tunnel called wormhole link. In this attack, an attacker at one location receives the packet and transmit it to another attacker which is very far-way, by a high speed wormhole tunnel in the network.

1) *Working*

Working of wormhole attack can be well explained by the following Fig. 3.

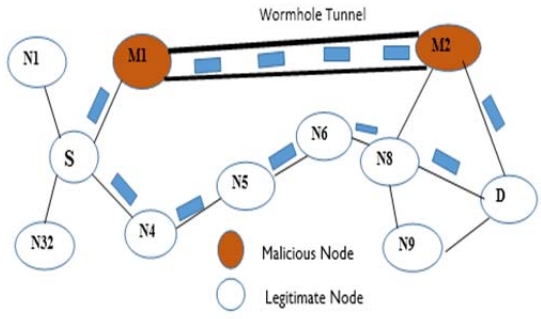

Fig. 3. Wormhole Attack in MANET

In this Fig. 3., Nodes S is Source node and Node D is destination Node when Node Source node S wants to communicate with the Destination Node D with the help of using routing protocols using MANET. Source Node S broadcasts the Route Request RREQ to its neighbour nodes .Here nodes M1 and M2 are two malicious nodes that are connected with each other by a high speed communication channel which is known as wormhole tunnel. Malicious node M1 is also a member of Source node S , as soon as M1 receives the RREQ from Node S it instantly sends RREP back to node S having route to destination node D with less number of hops. The source node S sends the packet through node M1 as it offers the shortest path. Then M1 node receives the packet from source node S and sends it to other malicious node M2 through wormhole tunnel. The malicious node can drop the packet or selectively forward the packet to destination

When the same Route Request RREQ that flows through legitimate nodes will arrive at destination. The destination node rejects these RREQ because it has already received the same Route request(RREQ) through the malicious node M2 .Hence it results in the disruption of routing protocols when the routing protocol are disrupted means whole network will be disturbed.

2) *Detection Metrics*

The following are metrics for detection of wormhole attack:

- Strength
- Attraction
- Robustness
- Packet delivery ratio
- Difference in the false path and true path.

Strength- The no of paths attracted by the attacker node by false advertisement. The strength of wormhole attack depends upon the traffic passing through wormhole channel. Increase in network traffic through wormhole link will increase the strength of attacker node [7].

Attraction- Attraction is directly proportional to the path length. If the path length offered by wormhole is small then attraction will be more which in turn increase the strength

of attacker node. But it the path length shows little improvement than actual path, attraction will be less, hence strength will be less.

Robustness- Robustness means capability of wormhole attacker to retain its effect without reducing the strength.
Packet Delivery Ratio- The Packet delivery ratio refers to the total no of packets received by the total no of packet sent.

Difference in fake path and true path- If the length of false advertised path is small (minimum no of hops) as compared to other actual paths. The difference in paths length can lead to detection of wormhole attack.

B. *Ad-hoc On-demand Distance Vector Protocol*

AODV [8] is a reactive protocol that does not maintain any routing information in routing table or maintain any periodic update. A node does not keep any other nodes information until it needs to communicate. Nodes maintain connectivity with their neighbour by using a technique (sending hello messages to neighbours). The routing table contains information of next hop to destination and sequence numbers that provides freshness of route. The AODV protocol uses three phases during communication between nodes are route discovery, route establishment and route maintenance. Control messages used in AODV Protocol are RREQ packet, RREP packet, Data Packet, RRER packet and their formats are given in below Table II, III, and IV respectively.

TABLE II
ROUTE REQUEST PACKET FORMAT

Source address	Broadcast id	Source Seq. No	Dest. Address	Dest. Seq. No	Hop count

TABLE III
REQUEST REPLY PACKET FORMAT [9]

Source Address	Dest. Address	Dest. Seq. No	Hop count	Life time

TABLE IV
ROUTE ERROR PACKET FORMAT

Unreachable Destination. IP address	Unreachable Destination Seq. No

IV. PROPOSED MODEL

Proposed model uses a mechanism to detect and avoid the wormhole attack in the Mobile Ad-hoc network where a wormhole attacker will get caught by its characteristic i.e., offering the source node fake route to destination. I named this mechanism as TAODV (Trapper Ad-hoc Distance Vector) model. This mechanism has some assumptions and is divided into three phases:

- Pre_AODV Wormhole Discovery Phase.
- Normal_AODV Route Establishment Phase.
- Post_AODV Wormhole Discovery Phase.

Assumptions:

- Wormhole attacker node does not act as source and target node.
- RREP will have one more field called Identity Field.
- Node will store next-nodes Information into log file.

A. *Pre_AODV Wormhole Discovery Phase*

In first phase, Bogus Route Request (RREQ) is broadcasted by source terminal with virtual destination (not existing). The malicious node (wormhole attacker node) when hears the Bogus RREQ, it will reply back RREP immediately offering shortest path to the target node. The malicious node have no interest in verifying whether virtual destination exists or not.

In this model, RREP sent against Bogus RREQ will contain one more field called Identity field, which stores the identity of node that sends RREP. The legitimate nodes will not reply to the Bogus RREQ because they do not have route to the virtual destination. In Fig. 4.

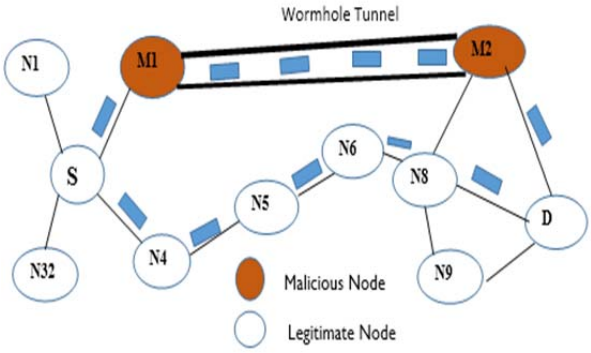

Fig. 4. Wormhole Attack in MANET

The identity of wormhole node will be stored in identity field. if there are more than one wormhole present then their identity are put in Black list and black list containing the wormhole nodes identity will be broadcasted as an ALERT message to all the nodes in the network. So that all the nodes come to know about wormhole nodes in a network. In the Figure: 4, we have two malicious nodes that form a wormhole link i.e., M1 and M2. When the source 'S' broadcasts the Bogus RREQ to its 1-hop neighbour node M1, N1 N4, N3 are its neighbours. Here, M1 as malicious node will send back the RREP immediately without knowing anything about the destination given in the Bogus RREQ and offers the minimum the hop-count route. Legitimate nodes N!, N3, N4 will not reply because they do not have route to the virtual destination.

B. *Normal AODV Route Establishment Phase*

Now the network is free from wormhole attack because every node knows the **Identity** of wormhole node (malicious node)**.** When nodes will send the True RREQ to neighbours. If the wormhole nodes sends the RREP, then its identity will be compared with the blacklist and its RREP will be rejected, hence AODV will be able to find the minimum hop count path from sender to destination which is without wormhole infected.

C. Post_AODV wormhole Discovery Phase

After making route with destination using AODV protocol, every node along the route after sending packet will also store next-node information (like delay in sending and receiving the packets) into a log file. If the delay is greater than threshold delay then wormhole is present and again phase 1 is started otherwise wormhole is not present.

Threshold delay can be calculated as an average delay. Fig. 5. Provides an overview of the security model and Fig.6. Provides the detailed security model for detection and avoidance of wormhole attack.

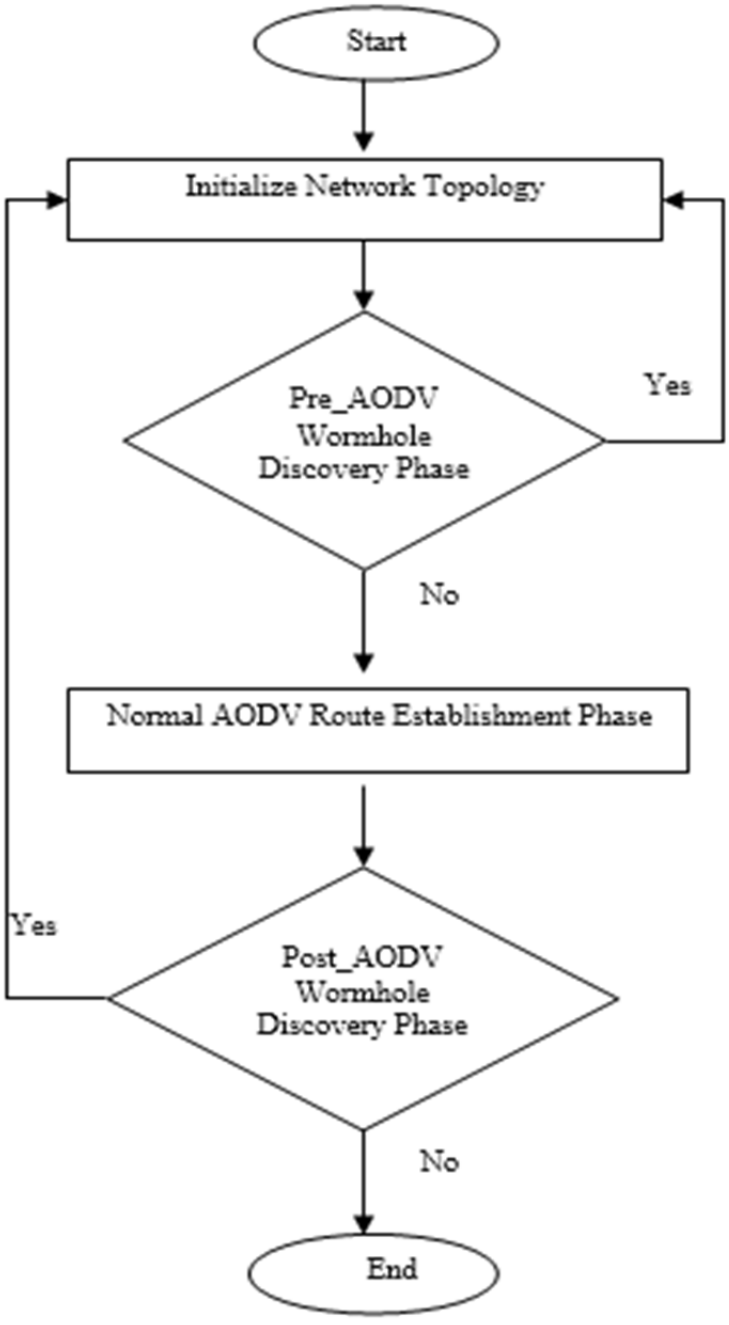

Fig. 5. Overview of TAODV model

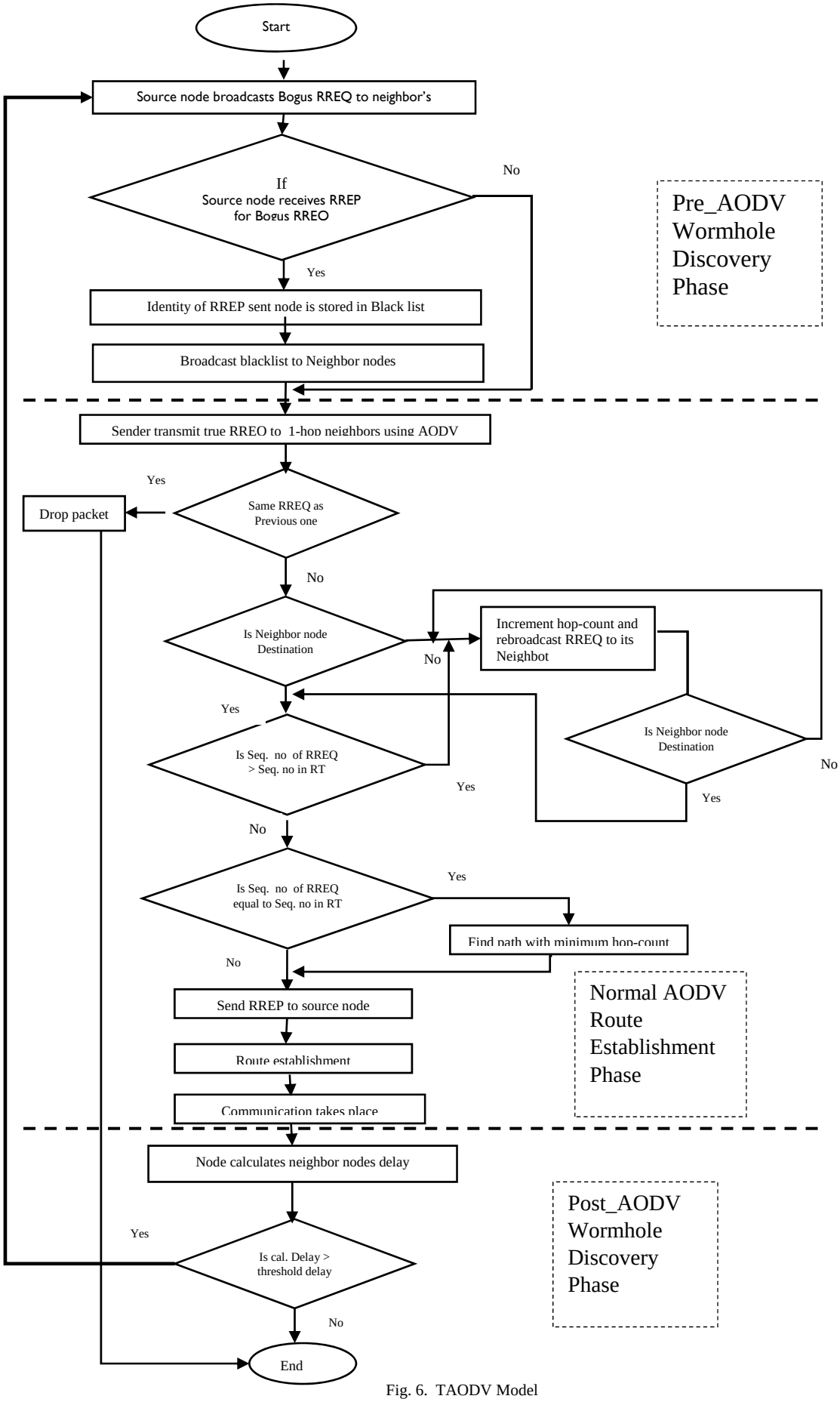

Fig. 6. TAODV Model

V. CONCLUSION AND FUTURE SCOPE

A. *Conclusion*

In this Paper, we have proposed a security model that will detects and avoids the wormhole attack in Mobile Ad-hoc Network and makes MANET free from Wormhole attack. This proposed model is simple and does not use any hardware. In the first phase, it will detect the malicious node in MANET by using Bogus RREQ and then remove the involvement of malicious node in the Network and in second phase apply AODV protocol for finding the shortest route to the destination. In the last phase, it again checks for presence of wormhole attack using average delay. If there is presence of wormhole attack then start from phase one again otherwise select the route for data transmission that was discovered in second phase.

B. *Future Enhancement*

In this Paper, the security model is provided to detect and avoid the wormhole attack in MANET. This proposed model should also be made to mitigate the following attacks.

- Black hole Attack
- Grayhole Attack
- Sinkhole Attack

Similarly, proposed security model should be improved to secure the MANET completely and that mechanism should be made by keeping following considerations in mind.

- Reliability
- Cost
- Mobility
- Use of limited resources

REFERENCES

[1] L.Sudha Rani, R.Raja Sekhar, " Detection and prevention of wormhole attack in stateless multicasting ", International journal of Science & Engineering Research Volume 3, issue 3, March – 2012. Page 1-5

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Tohoku University and Abbas Jamalipour, University of Sydney, "A Survey of Routing Attacks in Mobile Ad Hc Networks", Security in Wireless Mobile Ad Hoc Networks and Wireless Sensors, IEEE Wireless Communications, October 2007.

[3] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

[4] L. Hu and D. Evans. Using Directional Antennas to prevent wormhole attacks. In Proceedings of the Network and Distributed System Security Symposium (NDSS), Page 131-141, 2004.

[5] Ming-Yang Su, 2009"WARP: Wormhole Avoidance Routing Protocol by anamoly detection in mobile ad hoc network", Miang Chuan University, Taiwan, Elsevier.

[6] Shang Ming jen, Chi-Sung laih and Wen-Chung Kuo, 2009 "A Hop-Count Analysis Scheme for Avoiding Wormhole Attack in MANET", Sensors.

[7] Viren Mahajan, Maitreya Natu, Adarshpal Sethi, "Analysis of Wromhole Intrusion Attacks in MANETS", University of Dealware, IEEE, 2008.

[8] Charles E. Perkins and Elizabeth M. Royer," Ad-hoc On-Demand Distance Vector Routing", 2nd IEEE WorkShop on Mobile Computing System and Application (WMCSA'99).

[9] Laxmi Shrivasta, Sarita S. Bhadauria, G.S. Tomar, "Performance Evaluation of Routing Protocols in MANET with Different Traffic Loads", International Conference on Communication System and Network Techonologies IEEE 2011.