1-1-2011

Out-of-band wormhole attack detection in MANETS

Sana ul Haq

National University of Sciences and Technology (NUST), Islamabad, Pakistan

Faisal B. Hussain

National University of Sciences and Technology (NUST), Islamabad, Pakistan

DOI: 10.4225/75/57b53010cd8bb
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

OUT-OF-BAND WORMHOLE ATTACK DETECTION IN MANETS

Sana ul Haq, Faisal B Hussain
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
msis-6.sanaulhaq@mcs.edu.pk, faisalbashir@mcs.edu.pk

Abstract

Mobile Ad hoc Networks (MANETs) are prone to a variety of attacks due to their unique characteristics such as dynamic topology, open wireless medium, absence of infrastructure, multi hop nature and resource constraints. Any node in mobile ad hoc networks operates not only as end terminal but both as an intermediate router and client. In this way, multi-hop communication occurs in MANETs and thus it is a difficult task to establish a secure path between source and destination. The purpose of this work is overcome a special attack called wormhole attack launched by at least two colluding nodes within the network. In this paper we enhance AODV to detect and remove wormhole attack in real-world mobile ad hoc networks. In an out-of-band wormhole attack the communication between two malicious nodes is hidden from the rest of the nodes. This property is exploited by our proposed AODV-DRW protocol for the detection of wormhole attack.

Keywords
MANETs;AODV; Wormhole Attack, Secure Routing

INTRODUCTION

MANET (Mobile Ad hoc Network) is a type of wireless networks that have attracted most researchers towards them as MANETs provide better environment for ubiquitous computing that require no infrastructure without wired accessories (Corson, Maker & Cernicione, 1999).

Such networks can be deployed in a situation where exchange of critical information becomes necessary i.e. consider a military background with solders getting timely strategic and tactical information. Most of the existing routing protocols in MANETs i.e. AODV (Perkins, Belding Royer & Das, 2003), DSR (Jhonson & Maltz, 1996), DSDV (Perkins & Bhagwat,1994), are prone to a variety of attacks (Argyroudis & Mahony, 2003) that can degrade the performance of the whole network and thus pose direct threat to security of such networks, therefore we require solutions that if intruders enter our network, they can be timely detected and prevented before doing any unwanted task. The focus this paper is on the security of routing protocols in MANETs which are the target of the attackers for injecting malicious behavior. In this perspective we work on a special type of routing attack called wormhole (Jhaveri, Parmar, Patel & Shah, 2010) that exploit vulnerabilities in MANETs routing protocols.

Wormhole attack is a network layer attack. In a typical wormhole attack at least two colluding nodes in the network are located at different places that are not in direct communication range of each other i.e. one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing. In Figure 1, M1 and M2 are two colluding nodes. The malicious node M1 takes data near the source node then tunnels it to M2 placed near the destination node. Communication of data occurs via path having this low latency link all the times due to less number of hops.

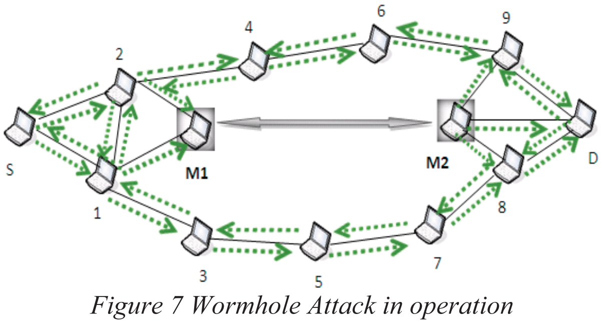

Figure 7 Wormhole Attack in operation

AODV is a reactive routing protocol commonly used in MANETs. In this paper, we have modified Ad hoc on-demand routing protocol AODV to detect and remove wormhole attack. In AODV, when a source node wants to establish a path with destination node, it creates Route Request packet and broadcasts to all its neighboring nodes that are in its communication range in a controlled fashion. All intermediate nodes rebroadcast the route request packet until it reaches to destination node in a controlled fashion. The destination node then creates route reply packet. Malicious nodes (which we call colluding nodes) using out-of-band channel communicate with each other, therefore route request packets broadcasted/unicasted from one malicious node to the other malicious node (near to the destination), are hidden from the rest of the network. We present a simple solution using the implicit characteristics of overhearing transmission A node can node can detect which neighboring nodes has forwarded a route request. AODV-DRW has been implemented over a MANET test bed where it has successfully detected malicious nodes launching wormhole attack under different scenarios.

The rest of the paper is organized as follows: In Section II, a brief description about the literature review has been provided. Section III identifies the problem statement. Section IV describes AODV-DRW in detail. Section IV has explained implementation of the AODV-DRW with possible scenarios and results. At the last we draw the conclusion for the paper and pointed out some potential works in the future.

LITERATURE REVIEW

A number of cryptographic, statistical, time and location based schemes have been proposed in existing literature (Azer, El-Kassas & El-Soudani, 2009). This paper is an effort to develop a light weight solution that not only detects but also removes wormhole attack in MANETs. Although, much of the research work has been done in this direction to overcome this attack with routing protocols in MANETs that performs simulation, however, less research in this context so far has been done to overcome this devastating attack using practical implementation.

In (Roy, Chaki & Chaki, 2009), the authors have proposed a cluster based scheme to avoid wormhole attack in MANETs that uses AODV as a routing protocol. The network is divided in to different clusters. Each cluster has cluster head which is selected dynamically in the inner layer and keeps routing information of all member nodes. There is also a cluster head in the outer layer responsible to pass on information to all member nodes in each cluster. The guard node located on the junction of clusters is responsible to monitor the malicious activity of member nodes. In case when a guard node detects any malicious activity of a node, it reports it to the cluster head in the cluster, which in response pass on the information to the cluster head in the outer layer which in turn informs all other nodes in the network about the malicious activity of the node. The results were collected using MATLab simulation.

In (Shang-Ming Jen, Chi-Sung Laih and Weh-Chung Kuo, 2009), a hop count based scheme is used to present wormhole attack. A route with a hop-count value, that is significantly smaller than the others, is most likely a wormhole. The proposed scheme uses simulator of C and Matlab to get results.

In (Panaousis, Nazaryan & Politis, 2009) a mechanism called AODV-Wormhole Attack Detection Reaction (AODV-WADR) uses a combination of cryptography and timing. Any node that wants to establish a route discovery starts a timer to calculate ATT (Actual Traversal Time). It suspects routes as of wormhole links when hop-count=3 and Actual Traversal Time > 6× (Node Traversal Time). The detection of wormhole attack up to 3-hops is justified due to the pattern of nodes, communication under the topology of AODV protocol. The suspicion is based on fact that attacker can use powerful signal to transmit the packet to distance greater than one hop but the time it calculates during this transmission can not be smaller than the time of IEEE 802.11b transmission in a single hop. To confirm the existence of wormhole attack, AODV-WADR uses Diffie-Hellman (DH) algorithm using AES cryptographic standards. It has the capability to handle open wormhole however in case of hidden wormhole AODV-WADR will not be efficient. Simulations were carried out using the network simulator NS-2.

In (Win & Gye, 2008) the authors have analyzed wormhole attack in ad hoc and sensor networks. Also an algorithm called DaW is presented that is based on establishing trust vector through neighbor monitoring together with link frequency analysis. In (Tun & Maw, 2008) Zaw Tun et al has proposed a method to detect wormhole attack using both Round Trip Time (RTT) and neighbor numbers. To detect wormhole attack each node first detects neighbor number (nn) in the network and then the source node observes the RTT between any two neighboring nodes on its path to destination. The source node then decides whether there exists a wormhole on the basis of any RTT values between any successive nodes. If the RRT value for any two successive nodes is found to be more than the normal, then it needs to check the value of nn. Now if nn value is also greater than average number of neighbors then it is certain that wormhole link is present.

In the recent paper of (Ming-Yang Su & Kun-Lin Chiang, 2010), the authors have proposed a solution to detect and discard malicious nodes of the wormhole attack based on the deployment of Intrusion Detection System

(IDS) in MANETs using on demand routing protocol i.e. AODV. The scheme uses packet loss as a metric to eliminate wormhole attack. The IDS nodes perform a mechanism called Anti-Wormhole Mechanism (AWM) that sniffs routing packets of the regular nodes that are in their transmission range. It is the responsibility of IDS nodes to determine any misbehavior of nodes in its vicinity. If any such thing happens it securely informs all other nodes in the network to isolate malicious nodes.

PROBLEM STATEMENT

A particularly severe attack called wormhole attack launched by two colluding nodes pose severe threat on MANETs routing. The attack is launched in our case by out-of-band channel. The colluding nodes are equipped with radio transceivers compatible with the mobile ad hoc network used. After establishing the tunnel the adversary may record/copy the data, do selective forwarding or aggregate large number of packets for packet analysis and decryption purposes. Even data encryption that is considered a perfect solution to handle attacks, does not provide a perfect solution because adversary captures the data and replays it through the wormhole tunnel at the other end near the destination node without decryption concerns. Colluding nodes force all other nodes to send data through them and make believe distant nodes that they are immediate neighbors of each other. The existence of such malicious nodes not only falsifies the route by disturbing the true topology of the network but also throughput of the network is badly affected. Locality based schemes to detect properties of an area such as temperature, pressure, concentration of toxins and pollutions are failed due to wrong decisions in such networks.

OPERATION OF AODV-DRW

Our proposed solution i.e. AODV-DRW not only detects but also removes the wormhole attack without the use of any special hardware. The proposed solution handles wormhole attack that is launched by two colluding node using out-of-band channel. Colluding nodes have the capability to communicate with all other nodes. All nodes are considered in promiscuous reception mode and are bidirectional. The colluding nodes use wireless capability that is of larger range than other normal nodes in the network.

The operation of the proposed solution for wormhole attack can be categorized in two steps:

- Detection of colluding node
- Removal of colluding node

Detection of colluding node

Normally in AODV (Perkins, Belding Royer & Das, 2003) all intermediate nodes that have no route to destination node rebroadcast RREQ forwarded by the originator of the RREQ. The source node/intermediate node keeps record of all the next neighbors from which it listen RREQ during rebroadcast. The following information is maintained by each node while broadcasting RREQ from originator node to destination node:

- Originator ID
- Originator Seq#
- RREQ ID
- Neighbor Node ID
- Timer

Maintaining this information at all nodes insure detection of any node conducting wormhole attack. As the colluding node uses out-of-band channel, its rebroadcast of RREQ is not listened by the neighbouring intermediate nodes, instead it forwards the RREQ to its colluding partner, and the forwarding neighbours of malicious node therefore do not listen to rebroadcast from the malicious node M1. As shown in Figure 1 in introduction section, the wormhole attackers establish a shortcut link between source node and destination node having least number of hops, therefore path having wormhole link will be selected, as RREQ packet reached by destination node in short period of time as compared to RREQs reached by other normal paths.

Removal of colluding node

Replying RREP packet on reverse route from destination node will follow the path having wormhole link. A node which receives RREP from a node that has no ID of that node is then considered as suspicious and is blacklisted. In Figure 1 source node "S" wants to send data to destination node "D".

The state transition diagram of our scheme is given in Figure 2 below:

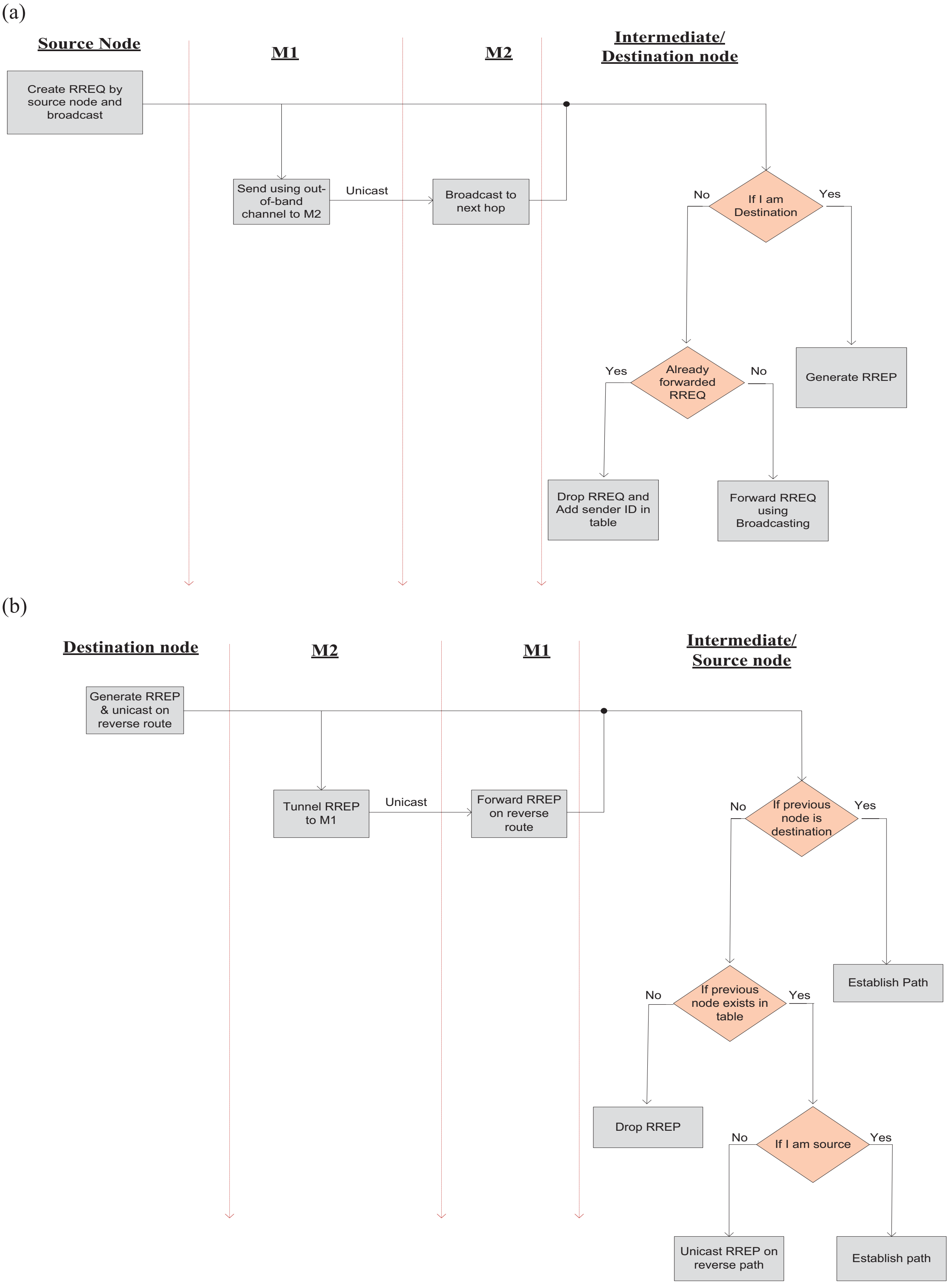
(a)
Source Node
M1
M2
Intermediate/ Destination node
Create RREQ by source node and broadcast
Send using out-of-band channel to M2
Unicast
Broadcast to next hop
No
If I am Destination
Yes
Generate RREP
Yes
Already forwarded RREQ
No
Drop RREQ and Add sender ID in table
Forward RREQ using Broadcasting
(b)
Destination node
M2
M1
Intermediate/ Source node
Generate RREP & unicast on reverse route
Tunnel RREP to M1
Unicast
Forward RREP on reverse route
No
If previous node is destination
Yes
Establish Path
No
If previous node exists in table
Yes
Drop RREP
No
If I am source
Yes
Unicast RREP on reverse path
Establish path

Figure 8 Event transition/State Transition Diagram. (a) RREQ (b) RREP

The working of our proposed scheme is summarized as:

I. RREQ is created by source node and broadcast it to all neighboring nodes which are in its communication range.

II. RREQ is rebroadcasted by all receiving nodes of RREQ until received by destination

III. The sending nodes of RREQ listen to the rebroadcast from all its neighbors, before discarding such RREQs they keep record of their IDs as next neighbor nodes. All normal nodes in MANETs get list of information as mentioned in the network.

IV. If receiving node of RREQ is malicious, its rebroadcast is not listened by normal neighboring nodes, because it unicasts RREQ to its colluding partner using out-of-band channel, thus all its neighbors will not hear from it and they will be unable to record their ID.

V. As shown in Figure 1, normally RREQ is reached to destination through route having colluding nodes due less number of hops and low latency as compared to other normal available normal routes.

VI. The RREP packet is created by destination node and is unicasted through the reverse route.

VII. The receiving node of RREP on reverse route will check if there exists an ID of the sending node of RREP in its maintaining information, if yes it will forward the RREP to next hop on reverse route towards the source node, otherwise, the receiving node regards that node as malicious and is blacklisted and future communication through that node is blocked.

VIII. Another alternative route having no malicious node is then selected for data communication.

IMPLEMENTATION OF PROPOSED SOLUTION

We have performed our experiments over Linux test bed having six PCs and two laptops. All these nodes are equipped with wireless capabilities. For implementation purpose we have used AODV-UU (n.d.) version of AODV that's compliment to AODV draft 13 (Perkins, Belding Royer & Das, 2003). Below are given the following two scenarios that depict how our proposed solution detects and prevents wormhole attack.

Scenario 1

We have more than one path in this scenario and wormhole path is of less number of hops than normal ones and malicious node is next to intermediate node as shown in Figure 3.

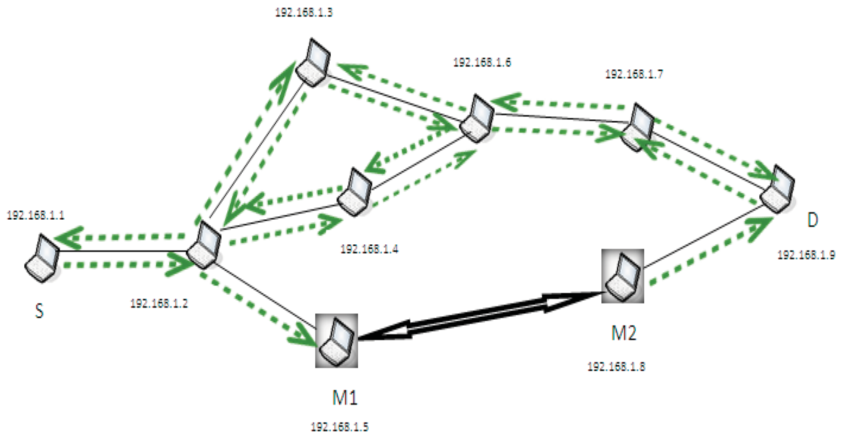

Figure 9 Scenario 1

As shown in the Figure 3 in this scenario, the ping request is instantiated from S to D. We have three alternative paths from S to D.

S<--->192.168.1.2<--->192.168.1.3<--->192.168.1.6 <--->192.168.1.7<--->D

S<--->192.168.1.2<--->192.168.1.4<--->192.168.1.<--->192.168.1.7<--->D

S<--->192.168.1.2<--->M1<--->M2<--->D

As node with IP address 192.168.1.2 detects and removes wormhole, the information shown in table 1 is maintained at this node during RREQ broadcast/rebroadcast during route discovery process:

Table 15 Neighbor Table of node with IP address 192.168.1.2

RREQ ID	Neighbor node ID	Timer (ms)	Originator ID	Originator Seq#
1	192.168.1.3	15000	192.168.1.1	0
1	192.168.1.4	15000	192.168.1.1	0
	No entry for M1			

Normally AODV follows path with out our scheme:

S<--->192.168.1.2<--->M1<--->M2<--->D due to small number of hops. However due to our AODV-DRW, the specified node does not have an entry of M1 node i.e. 192.168.1.5 and it is blacklisted and the paths are taken either as:

S<--->192.168.1.2<--->192.168.1.3<--->192.168.1.6<--->192.168.1.7<--->D or

S<--->192.168.1.2<--->192.168.1.4<--->192.168.1.6<--->192.168.1.7<--->D which are free of wormhole link. We perform the experiment for 10 times, and every time we got randomly the above paths. Thus our scheme detects and removes wormhole attack with 100% accuracy.

Scenario 2

The normal path is of larger number of hops as compared to path containing wormhole link and malicious node is next to intermediate node i.e. which received RREQ from source node and malicious node get RREQ from two different neighbors as shown in Figure 4.

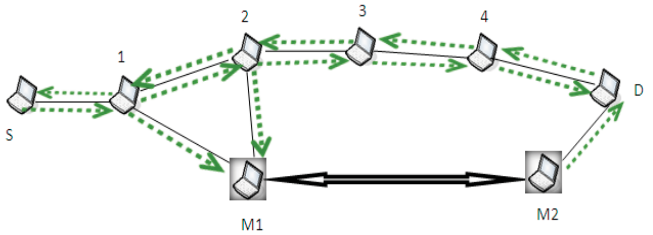

Figure 10 Scenario 2

In this scenario we have the following possible paths between source node S and destination node D:

S<--->1<--->2<--->3<--->4<--->D

S<--->1<--->2<--->M1<--->M2<--->D

S<--->1<--->M1<--->M2<--->D

Normal operation of AODV takes the path as:

S<--->1<--->M1<--->M2<--->D due to less number of hops and presence of wormhole link. However AODV-DRW does not select this path, instead it selects the path without wormhole as:

S<--->1<--->2<--->3<--->4<--->D

The experiment was performed for more than 10 times and every time we got the same result.

Scenario 3

The normal path and wormhole path are of same number of hops and malicious node is next to source node as shown in the Figure 5.

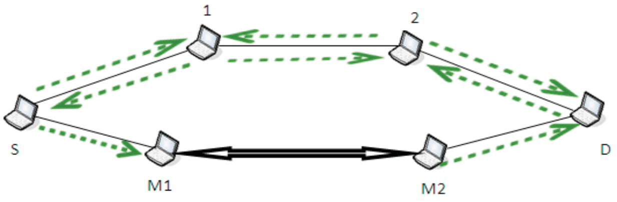

Figure 11 Scenario 3

Inevitably node S gets RREP through the path having wormhole link due to less latency, but source node blacklists node M1 as malicious due to its absence in neighbor list. Next time RREQ follows the path as:

S<--->1<--->2<--->D and it is then selected for data communication.

CONCLUSION AND FUTURE WORK

In this paper a practical solution called AODV-DRW, that use uses neighbor ID for detection and removal of wormhole attack with accuracy. The solution we have proposed is practical in the sense that it does not require any additional hardware. The memory and computational cost is reasonable enough to be supported by nodes in MANETs. Also instead of simulation we implemented it on test bed containing 8 nodes using existing hardware. Although our schemes detect and handle open wormhole attack successfully, however, incase of impersonation attack when a malicious node hides its identity with some normal node, our scheme fails, for which we require strong authentication scheme. In future we plan to embed some authentication scheme to overcome this deficiency in our scheme.

REFERENCES

Corson, M.S, Maker, J.P. and Cernicione, J.H. (1999). Internet-based Mobile Ad Hoc Networking. *IEEE Internet Computing,* pp. 63–70.

Perkins,C.E.,Belding Royer, E.M. and Das, S.R. (2003) . *Ad-hoc On-Demand Distance Vector (AODV) Routing.* Mobile Ad-hoc Networking Group, Internet Draft, draft-ietf-mendatory-00.txt.

Jhonson, D.B. and Maltz, D.A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, Kluwer Academic publishers, pp. 153/181.

Perkins, C.E. and Bhagwat,P. (1994). Highly Dynamic Destination-Sequenced Distance–Vector Routing (DSDV) for Mobile Computers, *Proceedings of the SIGCOMM 94 Conference on Communication Architecture, Protocols and Applications*, pp.234-244.

Argyroudis, P.G. and O'Mahony,D. (2003). "Secure Routing for Mobile Ad Hoc Networks", *IEEE Communications Surveys, the Electronic Magazine of Original Peer-Reviewed Survey Articles , 7*(3).

Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I. (2010). MANET Routing Protocols and Wormhole Attack against AODV, *International Journal of Computer Science and Network Security, 10* (4).

Roy, D.B., Chaki, R & Chaki, N. (2009). A New Cluster-Based Wormhole Intrusion detection Algorithm for Mobile Ad Hoc Networks. *International Journal of Network Security and its Applications (IJNSA),1*,(1).

Shang-Ming Jen, Chi-Sung Laih and Weh-Chung Kuo. (2009) ."A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors, ISSN 1424-8220, 9, 5022-5039; doi:10.3390/s90605022, 2009.

Panaousis, E.A., Nazaryan, L. & Politis, C. (2009). "Securing AODV Against Wormhole Attacks in Emergency Manets Multimedia Communications", Mobimedia'09, 2009, London, UK.

Win, K.S. & Gye,P. (2008). Analysis of Detecting Wormhole attack in Wireless Networks. *World Academy of Science, Engineering and Technology 48*.

Tun, Z & Maw, A.H. (2008). Wormhole Attack Detection in Wireless Sensor Networks. *World Academy of Science, Engineering and Technology 46*.

Ming-Yang Su and Kun-Lin Chiang. (2010). *Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes*. Springer Berlin / Heidelberg, vol: 6221, pages: 253-260.

AODV-UU.(n.d.). http://core.it.uu.se/AdHoc/AodvUU Impl

Azer, M., El-Kassas, S. & El-Soudani, M. (2009). A Full Image of the Wormhole Attacks: Towards Introducing Comlex Wormhole Attacks in Wireless Ad hoc Networks. *International Journal of Computer Science and Information Security (IJCSIS), 1*(1).