PERFORMANCE EVALUATION OF MODIFIED AODV AGAINST BLACK HOLE ATTACK IN MANET

Neha Kaushik, M.Tech Student
Ajay Dureja, Assistant Prof.
PDM College of Engineering for Women, B'Garh

Abstract

A mobile ad-hoc network is an infrastructure less network which consists of a number of mobile nodes that dynamically form a temporary network for the transmission of data from source to destination. They are composed of nodes that relay on each other to manage and for secure transmission of traffic due to lack of centralized administration. As MANETs become widely used, the security issue has become one of the primary concerns for all the times. One of the well known attack is the Black Hole attack which is most common in the on-demand routing protocols such as AODV.

In this paper, the proposed solution is to modify the AODV routing protocol in such a way that it can combat the cooperative Black Hole attack. The results show an effective increase in throughput and PDR and decrease in average end-to-end delay with a slight increase in routing overhead.

Keywords: MANET, AODV, Black Hole Attack, NS2

Introduction

A mobile ad-hoc network is categorized under infrastructure less network where a number of mobile nodes communicate with each other without any fixed infrastructure between them. Furthermore, all the transmission links are established through wireless medium [F.H. Tseng, Li-Der Chou, H.C. Chou 2011]. The functioning of MANET depends upon the trust and cooperation among the nodes in a network. Each node can act as a router or as a host for transmitting data packets to other nodes which are not in the range of direct transmission.

MANET is one of the recent active fields and has received marvelous attention because of its self-configuration and self-maintenance capabilities [Ujjwal Agarwal, K.P Yadav, Upendra Tiwari 2012]. MANET is widely used in military purposes, disaster area, etc where any infrastructured network is not possible to be laid. MANET offers greater flexibility, higher throughput, lower operating cost and better coverage than any other network because of collection of independent nodes [Pooja Jaiswal, Rakesh Kumar 2012].

The security of MANET is the primary concern now-a-days. The designing of routing protocols for Ad hoc network is a challenging task and secure ones are even more so. So far, in ad- hoc networking the routing problem have been studied in a non-adversarial network setting, assuming a trusted environment. Relatively, less research has been done in a more realistic setting in which an adversary may attempt to disrupt the communication [Yih-Chun, Adrian Perrig, David B. Johnson 2002].

Routing Protocols

The routing protocols in MANET are broadly divided into two categories – Proactive or Table-Driven routing protocols and Reactive or On-demand routing protocols. The third category is a combination of above two routing protocols known as Hybrid routing protocols.

In **proactive** or table-driven routing protocols, the mobile nodes broadcast their routing information to the neighbors on a periodic basis. Each of the nodes maintains a routing table which includes the information of next hop node, the destination node and the number of hops. In other words, all the nodes have to evaluate their neighborhood as long as the network topology has changed [F.H. Tseng, Li-Der Chou, H.C. Chou 2011]. The examples of proactive protocols are DSDV, OLSR, etc.

In case of **reactive** or on-demand routing protocols, the mobile nodes set up a route when there is a need to transmit the data packets from source to destination. The reactive routing protocols overcome the problem of increased overhead as in case of proactive protocols [Pooja Jaiswal, Rakesh Kumar 2012]. AODV and DSR are two main types of reactive routing protocols.

Hybrid routing protocol is a combination of proactive and reactive protocols. Most of hybrid routing protocols are designed as a hierarchical or layered network framework [F.H. Tseng, Li-Der Chou, H.C. Chou 2011]. ZRP and TORA come under the hybrid routing protocols.

Types Of Attacks

Mobile Ad hoc Networks are vulnerable to various types of attacks not from outside the network but also within the network itself [Gagandeep, Aashima, Pawan Kumar 2012]. The two major types of attacks in MANET are - internal attacks and external attacks.

Internal Attacks

These types of attacks make a direct impact on the nodes working in a particular network. Internal attacks may broadcast wrong type of information to other nodes. This type of attack is more difficult to be handled as compared to external attacks as these attacks are initiated by the authorized nodes in the networks, that can be a compromised node or a misbehaving node [Gagandeep, Aashima, Pawan Kumar 2012]. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized nodes in the network and then using them to launch attacks against the network. On the other hand, nodes can be classified as misbehaving if they are authorized to access the network resources, but fail to use these resources in a manner they should be [S. A. Razak, S. M. Furnell, P. J. Brooke 2004].

External Attacks

External attacks are the attacks which are launched by adversaries who are not authorized to participate in the network operations. These attacks aim to cause network congestion, denying access to specific network functions or to disrupt the whole network operations. Bogus packets injection, denial of service and impersonation are some of the attacks that are usually initiated by the external attackers [S. A. Razak, S. M. Furnell, P. J. Brooke 2004]. External attacks prevent the network from normal communication and producing additional overhead to the network [Gagandeep, Aashima, Pawan Kumar 2012]. External attacks are further classified into two types- Active attacks and Passive attacks.

Active Attacks

Active attacks are severe attacks on the network that prevent message flow among the nodes. Active attacks actively alter the data with the intention to obstruct the operation of the targeted networks [S. A. Razak, S. M. Furnell, P. J. Brooke 2004]. Active attacks may be classified as internal or external. Active external attacks are carried out by the outside sources that do not belong to the network. Internal attacks come from malicious nodes which are part of the network. Internal attacks are more severe and are hard to detect than external attacks [Gagandeep, Aashima, Pawan Kumar 2012].

Passive Attacks

These are the susceptible attacks of MANET. Passive attacks do not alter the data transmitted within the network, rather, include the unauthorized “listening” to the network traffic or data accumulation from the network. A Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of this type of attacks is difficult since the operation of network itself doesn’t get affected. In order to overcome such type of attacks powerful encryption algorithms are used to encrypt the data which is to be transmitted [Gagandeep, Aashima, Pawan Kumar 2012].

Network Layer Attacks In Manet

The security of the ad hoc networks heavily depends on the secure routing protocols, transmission technology and communication mechanisms used by the participating nodes of the network [Ujjwal Agarwal, K.P Yadav, Upendra Tiwari 2012]. The network layer protocols enable the MANET nodes to be connected with other node hop-by-hop. Every individual node takes the route decision to forward the packet, so it is very easy for malicious node to attack on such network [Gagandeep, Aashima, Pawan Kumar 2012]. Thus, security in network layer plays an important role in the security of the whole network.

A number of attacks on network layer have been identified and studied during the research. Our primary concern is on Black Hole Attack which affects the security of protocols like AODV.

AODV Protocol

Ad-hoc On-demand Distance Vector (AODV) routing protocol is a reactive routing protocol in which the network is established only when the source node desires to transmit data packets to the destination. The main distinguishing feature of AODV is the use of sequence numbers for every route entry. It broadcasts the RREQ, i.e., Route Request packet to its neighboring nodes to find a route to the destination node. The source increments its sequence number every time it generates a request packet and it has the recent sequence number of the destination which the source is aware of. The RREQ packet is forwarded to the other nodes until an RREP, i.e., Route Reply packet, comes from the destination or an intermediate node which has a fresh route to the destination. After receiving the RREP, the source forwards the data packets to destination via the intermediate node.

The figure shows the route discovery process from source to destination in AODV:

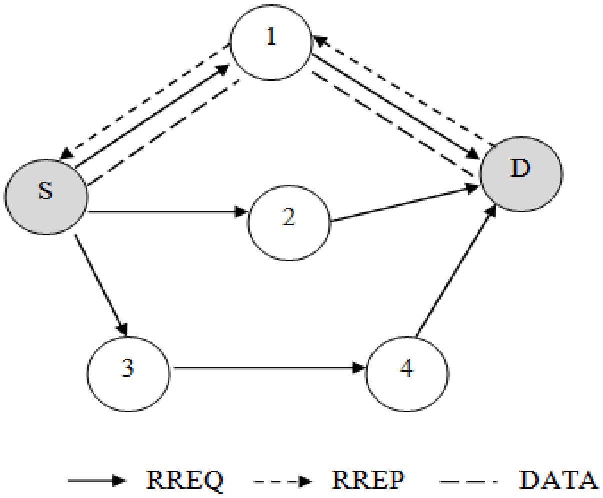

Figure 1. Route discovery in AODV

Black Hole Attack

A black hole attack is an active denial of service attack in which a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination [S.K. Chamoli, S. Kumar, D.S. Rana 2012]. A black hole can work as a single node as well as in a group. Since a black hole node does not need to check its routing table, it is the first one to respond positively to the RREQ [Pooja Jaiswal, Rakesh Kumar 2012]. Figure 3 below shows a black hole node 'X' which gives a false RREP to the source of having a fresh route to the destination. The source, then, routes all the data packtes towards the black hole node and this node absorbs all the data. Thus, the data packets are dropped and never reach the destination.

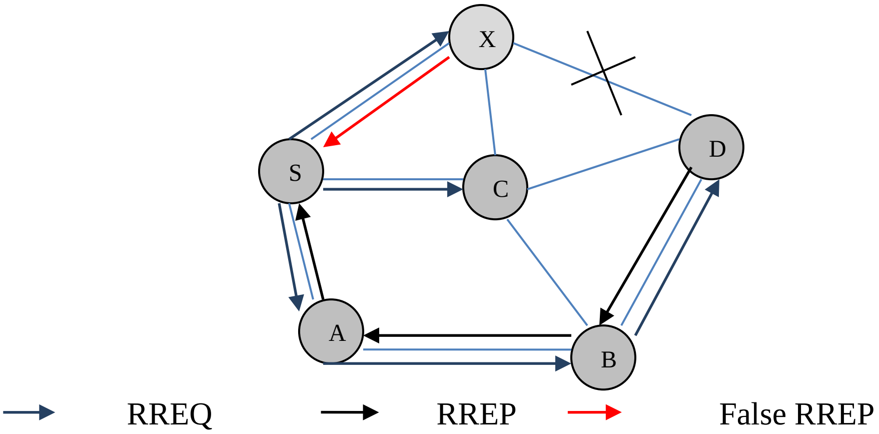

Figure 2. Black Hole Attack

Black hole attack is an active attack in case of AODV protocol. Since, AODV protocol has no security mechanisms, a malicious node can perform many attacks in the network just by behaving according to AODV rules [L. Tamilselvan, V. Sankaranarayanan 2007].

Related Works

A lot of research has been done to combat the black hole attack in MANET. Bo Sun et al. (2003) used AODV as their routing protocol. For defense against black hole attack, a neighborhood based method was devised to detect whether there exists any black hole attack or not and a routing recovery protocol to set up a correct path. In this scheme, a lower detection time and higher throughput are acquired and the accurate detection probability is also achieved.

Sanjay Ramaswamy et al. (2003) used a data routing information (DRI) table at each node and cross checking method to identify the cooperative black hole nodes in the network. The modified AODV routing protocol was used to achieve this methodology. The experiment results show that this solution performs better than other solutions. Mohammad Al-Shurman et al. (2004) provided two possible solutions to prevent the black hole attacks in MANET. The computer simulations show that the second solution can verify 75% to 98% of the route to the destination as compared to original AODV routing protocol. S. Kurosawa et. al (2007) proposed a detection scheme to detect the black hole attack by using dynamic training methodology in which the training data needs to be updated at regular time intervals. The simulation result shows the effectiveness of the scheme as compared to the conventional scheme.

L. Tamilselvan et al. (2007) proposed a solution based on the enhancement of original AODV routing protocol. The concept uses setting of the timer in the TimerExpiredTable for collecting the RREP packets from the other nodes after receiving the first reply. The table will store the sequence number of the packet and the receiving time of the packet in a Collect Route Reply Table (CRRT), looking for the timeout value based on the arrival time of the first RREP and judging whether the route is valid or not, based on the above threshold value. The simulation was taken using global mobile simulator (GloMoSim) which shows the increased packet delivery ratio with minimal delay and overhead. Nital Mistry et al. (2010) proposed modifications in the AODV protocol and justified the solution with appropriate implementation. The analysis show significant improvements in Packet Delivery Ratio (PDR) of AODV in presence of black hole attacks with marginal rise in average end to end delay. M. Umaparvathi et al. (2012) proposed a secure routing protocol, i.e., TTSAODV, an extension of AODV which can be used to protect the route discovery mechanism against black hole attack. The simulation result shows the better performance of the protocol than conventional protocol in terms of PDR and throughput. M. Medadian et al. (2012) proposed a method to combat cooperative black hole attack by waiting and checking the replies from all the neighboring nodes to find a safe route. The results show that the proposed protocol provides better security and performance in terms of PDR. Pooja Jaiswal et al. (2012) proposed a solution to prevent the black hole attack with the help of destination sequence number sent by the replying node. If a large difference between the sequence number of source node and intermediate node is accounted, then, node is declared malicious and its entry is discarded. The results show better performance in terms of PDR and end to end delay.

Proposed Solution

The proposed solution can be used to detect black hole nodes in the network and find secured routes for the transmission of data from source to destination. The solution involves two additional changes in the AODV protocol. First change is the addition of two parameters in the routing table of each node in the network. These parameters are DATA_PCK_SENT and DATA_PCK_REC.

DATA_PCK_SENT will count the total number of data packets sent to its next hop node, whereas, DATA_PCK_REC will count the data packets received from the next hop node.

Secondly, an additional routing table known as **Routing Information Table (RIT)** is to be maintained at source node. The RIT for source node is shown below –

Table 1. Routing Information Table

Sequence Number	Intermediate Node	Next Hop of Intermediate node

The source node stores all the RREP packets it receives according to their TIME_OUT values. When the time has expired, the source checks the RIT for the first sequence number received from the intermediate node. Generally, the first RREP is from the black hole node. Thus, the source checks its initial routing table that whether it has sent or received any data from the intermediate node or not. When it finds that it is a genuine node, the source forwards the data to this node. Otherwise, if the source finds that intermediate node is unreliable, then, it sends a further RREQ packet to the next hop node of intermediate node to cross check whether this node has sent or received any data from the intermediate node. If there is a positive reply from the next hop node, source forwards the data packets to the intermediate node. Otherwise, the source marks its entry as black hole node and eliminates its entry from RIT and checks the next RREP entry in the routing information table.

The purpose behind these two modifications is to increase the performance of AODV and eliminate the problem of Black Hole attack in MANET. The addition of RIT at source helps the source node to check the reliability of the intermediate node and then forwarding data to this node.

The algorithm for modified AODV to detect and prevent black hole attack in MANET is given below –

```
Source Node broadcasts RREQ
Source Node receives RREP
IF (RREP is from Destination or reliable node {
    source routes the data packets
}
ELSE {
    Do {
        Send further RREQ to the next hop node of intermediate node from RIT
        receive RREP from next hop node
        IF (Intermediate Node is a reliable node) {
            source routes the data packets to intermediate node
        }
        ELSE {
            Intermediate node is a Black Hole node
        }
    } WHILE (Intermediate node is a reliable node)
}
```

Simulation Results

The simulation is done using NS2, i.e., Network Simulator version 2. NS2 is an event driven simulation tool that is used to study the dynamic nature of communication networks [Introduction_to_network_Simulator_NS2, Teerawat Issariyakul, Ekram Hossain].

The parameters used in the simulation are shown below –

Table 2. Simulation parameters

Parameters	Values
Network size	700 m * 700 m
Number of Nodes	20 – 60
Max. speed/mobility	10.0 m/s
Pause Time	2.0 s
Traffic Model	CBR
Routing Protocol	AODV
Simulation Time	100 s

The metrics which are used in evaluating the performance of protocol are:

1. Packet Delivery Ratio: It can be defined as the ratio of total number of data packets delivered to the destination to the total number of data packets generated by the source. It is calculated as –

P = (number of packets received) / (number of packets sent) * 100

A decrease in PDR is seen when there is a black hole attack on AODV. In the results below, we can see that there is an effective increase in the PDR of modified AODV.

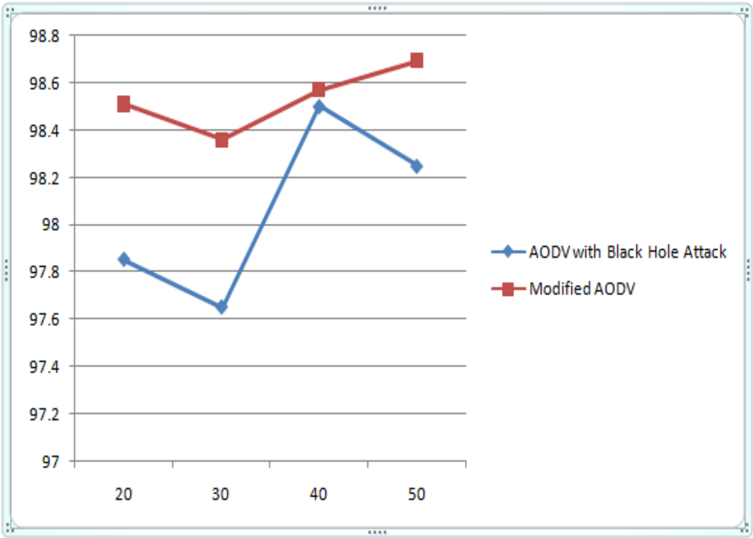

Figure 3. PDR Vs no. of nodes

2. Average Throughput: It is the average rate of successful message delivery over a communication channel. It is measured in data packets per second.

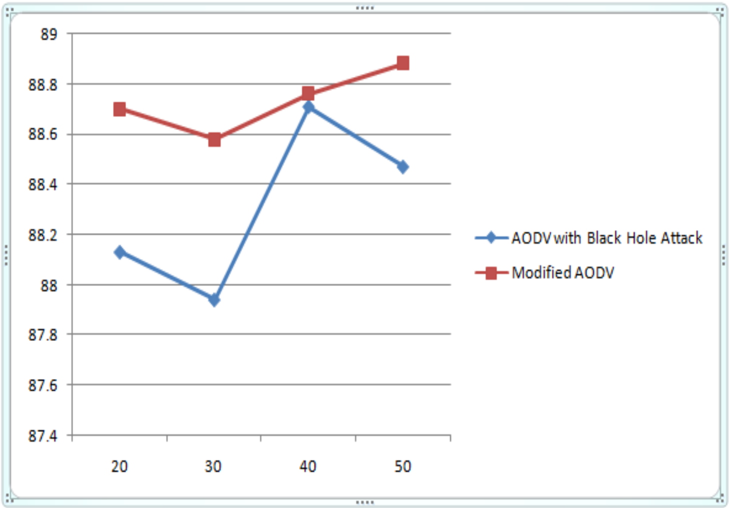

Figure 4. Avg. throughput Vs no. of nodes

The result in the figure clearly shows that the modified AODV has better throughput.

3. Average End-to-End delay: It is the average delay between the sending of packets by the source and its receipt by the receiver.

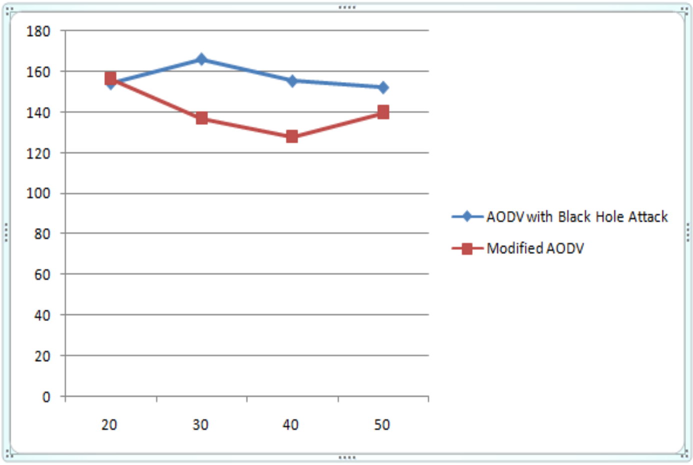

Figure 5. end to-end delay Vs. no. of nodes

4. Routing Overhead: It is defined as the ratio of sent routing packets over the received data packets.

The figure below shows a slight increase in the routing overhead of proposed AODV protocol.

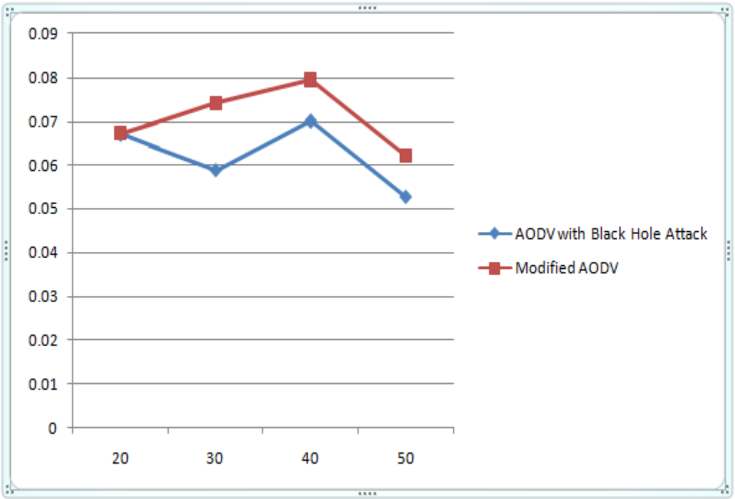

Figure 6. Routing overhead

Conclusion And Future Work

Mobile ad hoc networks have gained attention due to its self-configuration and autonomous capabilities. Due to various difficulties in designing of secure routing protocol, MANET has always been an important concern. In this paper, our main concern is of Black Hole Attack which is an active denial of service attack in AODV protocol which takes all the data packets from the source and absorbs them. The proposed solution which can be mounted against black hole attack in MANET. The proposed method can be used to identify black hole nodes in the network and finding secured routes for transmission of data.

As future work, we try to develop simulations to decrease the routing overhead over the network.

References:

F.H. Tseng, Li-Der Chou, H.C. Chou, Human-centric Computing and Information Sciences 2011, “A survey of Black Hole Attacks in wireless mobile ad-hoc networks”.

Gagandeep, Aashima, Pawan Kumar, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”.

Teerawat Issariyakul, Ekram Hossain, Introduction_to_network_Simulator_NS2.

L. Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANET", the 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007).

M. AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004).

M. Medadian, K. Fardad, European Journal of Scientific Research, Vol. 69 No. 1 (2012), “Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol”.

Mistry N, Jinwala DC, IAENG, Zaveri M (2010) “Improving AODV Protocol Against Blackhole Attacks”, Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.

M. Umaparvathi, D.K. Varughese, European Journal of Scientific Research, Vol. 72 No. 3 (2012),”Two Tier Secure AODV against Black Hole Attack in MANETs”.

Pooja Jaiswal, Rakesh Kumar, International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.2, No5, October 2012, “Prevention of Black Hole Attack in MANET”.

S. A. Razak, S. M. Furnell, P. J. Brooke, “Attacks against Mobile Ad Hoc Networks Routing Protocols”,2004.

Sun B, Guan Y, Chen J, Pooch UW (2003) “Detecting Black-hole Attack in Mobile Ad Hoc Networks”, Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, U.K., 22-25 April 2003.

Sweta Jain, Jyoti Singhai, Meenu Chawla, International journal of Ad hoc, Sensor & Ubiquitous Computing Vol. 2, No. 3, 2011, “A Review Paper on Cooperative Blackhole and Grayhole Attacks in MANETs”.

S.K. Chamoli, S. Kumar, D.S. Rana, International Journal of Computer Technology & Applications, Vol. 3 (4), 2012, “Performance of AODV against Black Hole Attacks in MANETs”.

S. Kurosawa, H. Nakayama, and N. Kato, “Detecting black hole attack on AODV based mobile ad-hoc networks by dynamic learning method, ”*International Journal of Network Security”*, pp. 338–346, 2007.

S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA.

Ujjwal Agarwal, K.P Yadav, Upendra Tiwari, International Journal of Research in Science and Technology, 2012, vol. no. 1, issue no. IV, Jan-Mar, “Security Threats in Mobile Ad hoc Networks”.

Yih-Chun, Adrian Perrig, David B. Johnson, “Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks”,sparrow.ece.cmu.edu/~adrian/projects/securerouting/ariadne.pdf, 2002.