Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.217 – 223

RESEARCH ARTICLE

A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets

Swati Pokhariyal[1], Pradeep Kumar[2]

[1]M.Tech Student, CSE Department, JSS Academy of Technical Education, Noida(UPTU), India
[2]Assistant Professor, CSE Department, JSS Academy of Technical Education, Noida(UPTU), India
[1] swatipokhariyal@gmail.com; [2] pradeep8984@jssaten.ac.in

Abstract— Mobile Ad-hoc network (MANET) is a self-configuring and infrastructure-less network of mobile nodes which are connected to each other without wires. Each node in a MANET moves freely and independently in any direction and this leads to a frequent change in their location and dynamic topology of the network. The structure-less architecture of Mobile Ad-Hoc Networks (MANETs) allow various attacks and vulnerabilities in the network. Blackhole / Grayhole are such type of DoS attacks that pose a threat to the working of MANETs. Blackhole / Grayhole attacks both correspond to dropping of packets which are being transmitted in the network which does not allow safe data communication in MANETs. It's difficult to detect these attacks by using any cryptographic measures because they do not create any separate packets. In this paper we proposed a technique that helps in searching the malicious node in the network and removing it completely. The Ad hoc On-Demand Distance Vector (AODV) routing protocol used in this scheme for Blackhole / Grayhole detection is a type of on-demand routing protocol in which the route discovery process starts only when packet transfer is required between a pair or source and destination. Our proposed work has been designed keeping in mind the packet dropping functionality of both the attacks and thus is able to detect and remove both Blackhole and Grayhole attacker nodes from the network.

Keywords— MANET, Blackhole Attack, Grayhole Attack, AODV, Backbone Node

I. INTRODUCTION

A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes that are capable of communicating with each other. MANETs are networks lacking any centralized monitoring and consist of network topology which changes dynamically [2]. They have a large number of potential applications and are widely used for military purposes such as connecting soldiers or other military units to each other on the battlefield or creating sensory arrays with thousands of sensors. Ad hoc networks allows creation of a network in situations where creating the infrastructure would be impossible or very expensive. In contrast to any network with a fixed infrastructure, mobile nodes in ad hoc networks are not able to communicate with the help of access points. Each mobile node acts as a host when we request/provide information from/to other nodes in the network, and acts as router for route discovery and maintenance for other nodes in the network.

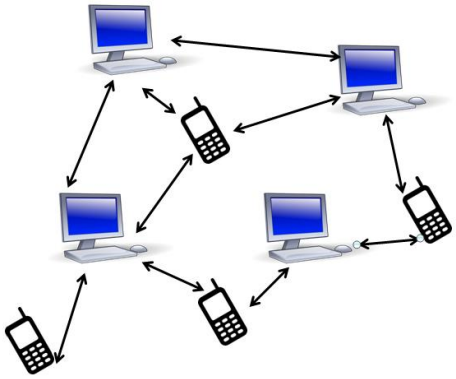

Fig 1: Figure representing the inter connection of different nodes in MANETs

Due to the absence of a centralized administration there is an unclear line of defence in ad hoc networks. This makes MANETs very vulnerable to attacks and other possible threats. Security in MANETs is thus a very crucial area of research. There exist various types of attacks which are being studied and efficient methods are being introduced to detect such malicious nodes present in the network. Out of all the existing threats in MANETs, the Denial of Service attack (DoS) is the most common and the most dangerous attack, where a particular malicious node does not allow services to be provided to other nodes and disrupts the smooth functioning of the network. The two most common types of DoS attacks in MANETs are Blackhole/Grayhole attacks.

A. Blackhole Attack

In the Blackhole attack, the malicious node on receiving a route request from any node, falsely replies immediately with the shortest path to the destination. This way the source considers the path through the attacker as the shortest path and uses the path through attacker for all data flow between the source and destination. The attacker node can then drop all the traffic passing through it or selectively drops traffic; hence acts as a Blackhole in the network. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. As shown in Figure 2, the Black hole node (BH) drops all the packets received by it without forwarding it to its next hop node Node2 (N2).

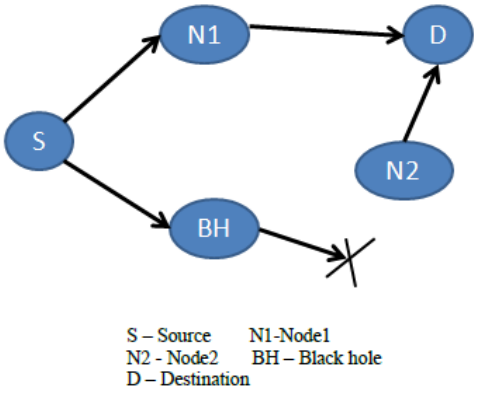

Fig. 2: Black Hole Attack in Mobile Ad-hoc Network

B. Grayhole Attack

In Grayhole attack [1] a malicious node trashes to precede certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. A Grayhole node in the network exploits the AODV protocol to announce itself as having a valid route to destination node, with the intension of interjecting or humiliating packets, even though route is counterfeit. The process of finding Grayhole node is a very challenging task. In some cases Grayhole attack is also called as node misbehaving attack. The Grayhole attack looks for to unsettle the network without being detected by the security measures in place. A Grayhole attack is a modified form of Blackhole attack in which a node initially behaves non-maliciously but later turns malicious after gaining initial trust of other nodes; hence prevents itself from being detected easily. Due to this behaviour, it is very hard to figure out such kind of attack. Figure 3 below represents node 6 as the Grayhole node which drops all the packets coming from source.

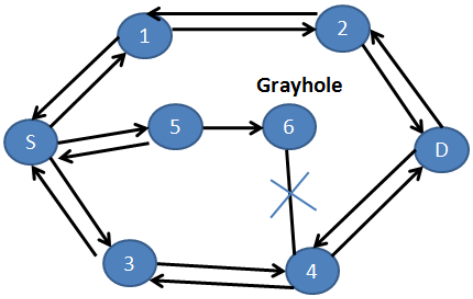

Fig 3: Gray Hole Attack in Mobile Ad-hoc Network

The rest of the paper has been categorised in different sections. Section II contains the literature review describing the previous methods implemented for detection of such type of attacks. In Section III, our proposed algorithm is discussed for detection and elimination of Grayhole/Blackhole attack present in the network. Theoretical analysis of the proposed scheme along with the conclusion and future work has been explained in Section IV.

II. RELATED WORK

Piyush et.al [9] proposed a solution which includes source and destination nodes performing end-to-end checking to determine safe delivery of data packets to the destination node. They have also proposed a concept of network of reliable nodes forming a backbone node for detection of malicious node in the network. If at any point the end-to-end check fails then this backbone network initiates the detection process for detecting the presence of any malicious nodes. This algorithm has a drawback that it works on assumption that a particular node in the network has the count of trusted neighbour nodes is always greater than the count of malicious neighbour nodes. This may not be true in many scenarios. If at any particular point of time, the number of malicious nodes in the neighbourhood exceeds the trusted nodes then this solution becomes vulnerable.

Another mechanism has been proposed by Sukla et. al [10] in which the source sends a PRELUDE message to the destination node before sending the actual block of data. This makes the destination aware that a communication is about to take place. The flow of the traffic in the network is monitored by the neighbouring nodes and a POSTLUDE message is sent back to the source node from the destination node which contains the number of packets received at the destination. If the number in the POSTLUDE message is less than the threshold value or acceptable range then the detection process is initiated. Based on the response from all the monitoring nodes, the malicious node is detected and is later eliminated from the network. The drawback of this method is the increased routing overhead due to the additional of routing packets.

Ramaswamy et al [11] proposed a method for detection of cooperative Blackhole nodes cooperating in a group in MANETs. They proposed a new concept of Data Routing Information (DRI) table along with Cross Checking method for detecting multiple Blackhole nodes in the network. The solution involved two bits of additional information provided by each node which responds to the RREQ packet sent by the source node. The DRI table contains values '1' which denotes TRUE and '0' for FALSE. The table contains a Node field and each node corresponds to two fields - (1)"From" which denotes information on routing the data packet from the node mentioned in the Node field and (2) "Through" which denotes information on routing of data packet through the node (present in the Node field). Each intermediate node passing the RREQ packet sends the ID of the next hop neighbour and its DRI entry to the source node. If RREP is received from a reliable node then the data is sent through that path, otherwise the source checks if its intermediate node and its next hop neighbour are reliable with the use of values existing in the DRI table and the cross checking mehod to detect the Blackhole node. This solution, however, fails to detect the presence of Grayhole nodes which alternate thier status from malicious to trusted node and vice versa.

G. S. Bindra et al [8] have used the concept of DRI and have proposed a mechanism for detection and elimination of co-operative Blackhole and Grayhole attacks where each node in the network maintains an EDRI (Extended Data Routing Information) table. EDRI table is used for malicious node detection and also provides additional fields which maintain information about all previous malicious nodes detected in order to reduce the Blackhole/Grayhole behavior. The proposed technique is also able to handle multiple instances of attacks present in the network in addition to detection of cooperating nodes and provides a secure path from source to destination.

Vani A. Hiremani and Manisha Madhukar Jadhao [6] have modified the EDRI table and proposed a Modified Extended Data Routing Information (MEDRI) table which contains additional fields-'Packet size at source', 'Packet size at destination' and 'Result'. These extra fields in the MEDRI table help in verifying whether a data packet has been recieved at the destination completely or partially. It provides a solution to the packet routing problem in MANETs along with providing a secure path for data transfer.

Sarita Choudhary & Kriti Sachdeva [7] have proposed a technique which uses the concept of Backbone nodes consisting of trusted nodes present in the network. For establishing a secure path the source node requests the Backbone nodes for an unused IP address and a RREQ is sent to the destination and the unused IP adress simultaneously. The Blackhole / Gryhole nodes present in the network tend to reply to the RREP for the unused IP also. On recieving a reply from the unused IP, the source initialises the detection process for detection and removal of these malicious nodes from the network.

Jhaveri et al [3][4] have proposed a Reliable-AODV (R-AODV) which is a modification of existing protocol which improves the route discovery process of AODV by eliminating Blackhole / Grayhole nodes from its path. They use the concept of Peak value which is calculated by adding these parameters - (1) Number of sent out RREQs, (2) Number of received RREPs and (3) Routing table sequence number. This Peak value is then compared with the destination sequence number for Blackhole / Grayhole detection. This method helps in detection and isolation of multiple attacker nodes during the route discovery process resulting in a secure and short path between source and destination.

III. OUR ALGORITHM

In this paper we propose an algorithm that detects and eliminates both Blackhole as well as Grayhole attack in the network.
In our algorithm, we consider 3-4 Candidate Nodes out of which the node having the highest residual energy is considered as the Backbone Node (BBN). The other nodes are in passive form and BBN work is performed by one active node. If at any point the energy of the active node decreases then it transfers control to the next candidate node having the max energy and all other nodes become passive. The tables used for detection are shared among all the candidate nodes and only the active node acting as the BBN node has read/write access to these tables. Other passive nodes have only read access to these tables. Thus, at one point of time, there is only one active node acting as the BBN and performing the detection activities. This reduces the overhead on the network as we do not need to establish a connection between all the other candidate nodes and with the help of a single BBN node the computation process increases leading to faster and accurate detection.

The protocol used in our proposed work is AODV protocol [12] and the basic 4 steps of the detection mechanism are as follows:

A. Request for RIP:

An IP in the network that is unused and is not provided to any node in the network is called a Restricted IP [7]. The source sends a request for Restricted IP (RIP) to the Backbone Node (BBN). The BBN contains a pool of RIPs and randomly selects and provides RIP to sender node.

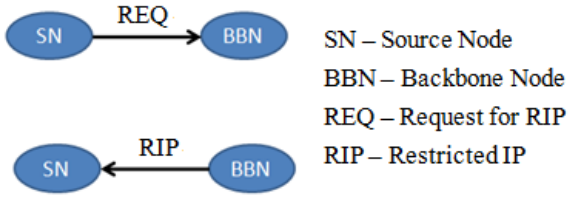

Fig 4: Source sends RRIP to BBN and the BBN replies by providing the RIP to the source node

B. Route Discovery:

On receiving the RIP, source sends Route Request (RREQ) to RIP. If we receive a reply from RIP then that Route Reply (RREP) contains a Blackhole/Grayhole node. For accurate identification of the attacker node in the path, we introduce a new field – "Origin" in RREP using the reserved bits of the packet. This field contains the ID of the node which has sent the RREP. When the source receives RREP from RIP it then sends the Node ID present in the Origin field as a vote to the BBN as a potential attacker node and initiates the detection process.

C. Attacker Node Detection:

As shown n figure 5 above, on receiving RREP from RIP, sender sends a dummy data packet on that path and enters into promiscuous mode. It checks whether its next hop neighbour (NHN) is correctly forwarding the dummy packet to the next node in the RREP. If the NHN is working properly, the source node stops its promiscuous monitoring and allows its NHN to start monitoring for the next node. Any node dropping the dummy packet at any point of time in the path is detected as a potential Blackhole/Grayhole Node and its Node ID is sent to the BBN as a vote. The flowchart representation of detection at source node is provided in Figure 5. Each Node ID received at the BBN as a vote is added to the Malicious Node table which is maintained at the BBN. This table contains two fields – Node ID and Count value for each node as shown as an example in Table 1 below.

Table 1: Structure of the Malicious Node table maintained at the BBN node

Node ID	Count
A	1
B	1
C	3
E	1

Whenever a new node is added to the Malicious Node table its count value is set to 1 and if a node is already present in the table then we increase its count value by 1 every time that node is detected as a potential attacker node in the network.

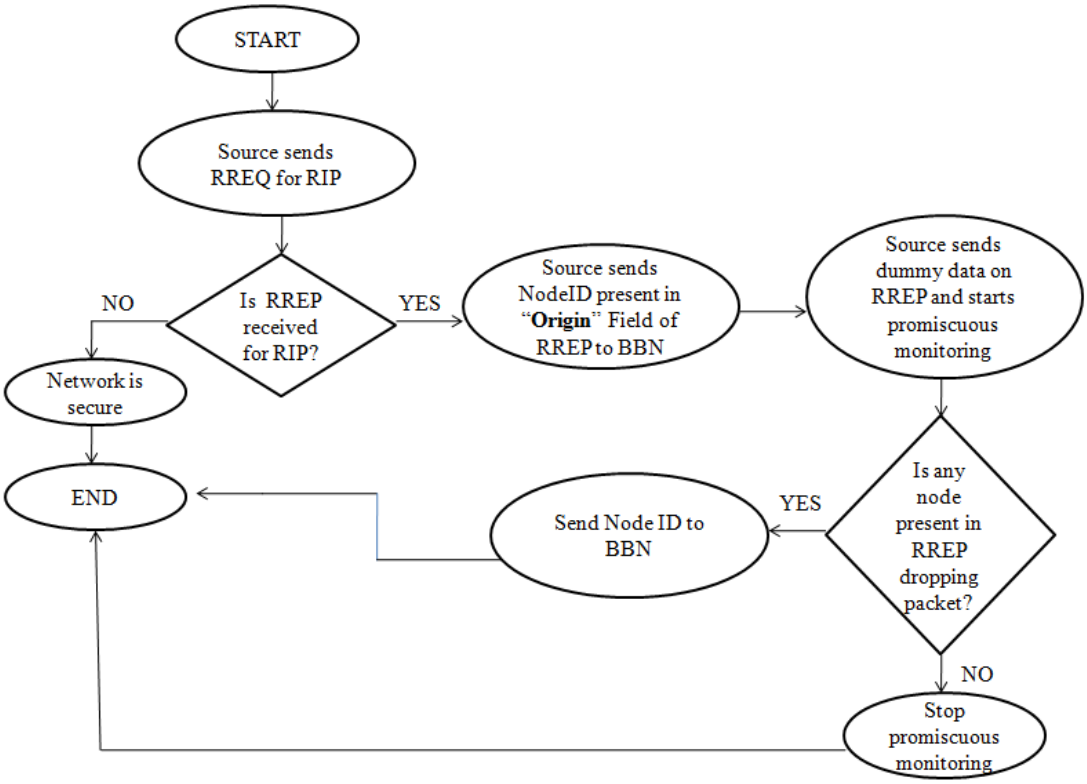

Fig 5: Flowchart representing detection process at Source node

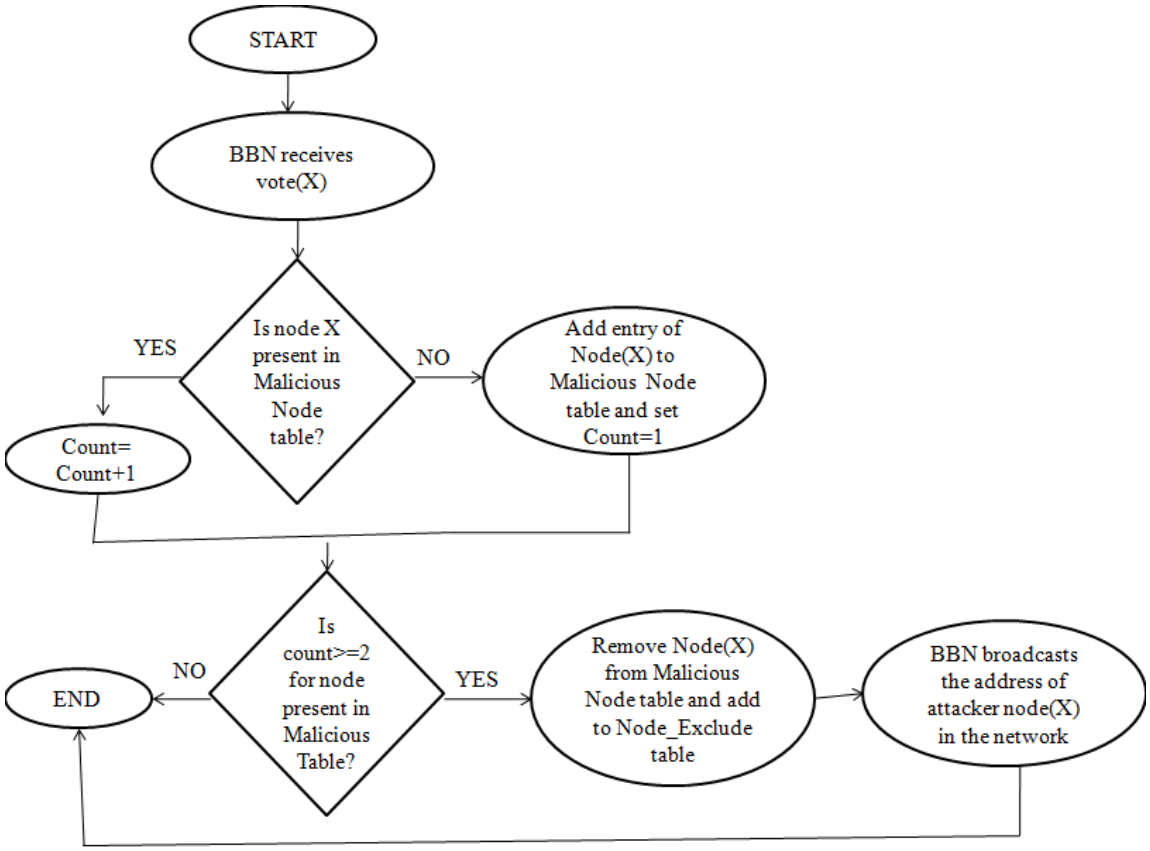

Fig 6: Flowchart representing detection process at BBN node

D. Blackhole/Grayhole Node Elimination:

If any node present in the Malicious Node table whose count value increases a threshold value then that node is detected as a Blackhole/Grayhole Node and its node ID is removed from the Malicious Node table and is added to the Node_Exclude table maintained at BBN. This node ID is then broadcasted to all the other nodes in the network and every other node marks this Node ID as an attacker node in their routing tables for secure routing. With the help of the count value and threshold value we are able to remove false positives from our results and we are able to detect the accurate attacker nodes from the network and eliminate them. As shown in the above Table 1, the Node C has its count value exceeding the threshold value (say threshold=2). So in this case the Node C will be added to the Node_Exclude table and eliminated from the network as shown in Table 2 below. The detection process at BBN node is explained in flowchart in Figure 6.

Table 2: Structure of the Node_Exclude table maintained at the BBN containing Node ID of attacker node eliminated from network

Node ID
Q
C

IV. CONCLUSION & FUTURE WORK

Security issues have been overlooked while designing routing protocols for ad-hoc networks. Through default AODV protocol, it is easier to breach the security of a MANET. AODV is susceptible to many DoS attacks including Grayhole and Blackhole attacks. In this paper, we investigated some of the existing solutions for these attacks and proposed a novel approach to counter these attacks that efficiently detects both Blackhole and Grayhole nodes in the network and eliminates them from all future communications to increase network security. Instead of removing the entire path containing the malicious node, our work focuses on removal of only the attacker node. Theoretical analysis shows that our approach would greatly increase PDR and also deals with the problem of false positive [5]. With the double verification technique false positives are removed to a large extent and the attacker nodes are detected with greater accuracy. We have also dealt with the single node failure problem by timely checks on the energy levels of the Backbone node. At any point of time if the energy of the Backbone node reaches

below threshold it transfers control to the next highest energy node in the network leading to smooth functioning of the detection process. As a part of our future work we intend to implement our work using NS-2 and analyse its performance on various parameters of throughput, end to end delay etc.

ACKNOWLEDGEMENT

The author would like to thank the faculty of Computer Science and Engineering Department, JSSATEN for their valuable guidelines and support.

REFERENCES

[1] Deepali et al, "*Review of Defense Mechanism against Gray Hole and Black Hole Attack in MANETs*", International Journal of Engineering Research & Technology (IJERT), Volume 3, Jan 2014, pp. 885-891

[2] Madhuri Gupta & Krishna Kumar Joshi, " *An Innovative Approach to Detect the Gray-Hole Attack in AODV based MANET*", International Journal of Computer Applications, Volume 84 – No 8, December 2013, pp 44-50

[3] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "*A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks*", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.556-560.

[4] Rutvij H. Jhaveri, "*MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs*", IEEE International Conference on Advanced Computing & Communication Technologies, 2013, pp. 254-260

[5] Harsh et al, " *Cooperative Blackhole/ Grayhole Attack Prevention in Mobile Ad hoc Network: A Review*", International Journal of Computer Applications, Vol 64, Feb, 2013, pp. 16-22

[6] Vani & Manisha Madhukar Jadhao, "*Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET*", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE),IEEE, 2013, pp. 944-948

[7] Sarita Choudhary, Kriti Sachdeva, "*Discovering a Secure Path in MANET by Avoiding Black/Gray Holes*", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012, pp.88-93

[8] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "*Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs*" IEEE International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia.

[9] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "*Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks*", 2nd international Conference on Ubiquitous information management and communication, 2008, pp.310-314.

[10] Sukla Banerjee, "*Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks*", World Congress on Engineering and Computer Science , October 2008, pp. 337-342

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "*Prevention of cooperative black hole attack in wireless ad hoc networks*", In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03),Las Vegas, Nevada, USA, 2003, pp. 570–575.

[12] Charles E Perkins & Elizabeth M Royer, "*Adhoc On Demand Distance Vector Routing*", WMCSA '99 Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, 1999, pp 90-101

