ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

Enhanced Cooperative Bait Detection Scheme to Prevent Malicious Node Launching Black Hole/Worm Hole Attacks in Mobile Ad Hoc Network

D.Abinaya[1], B.Senthil Murugan., M.E[2]

PG Student [Applied Electronics], Dept. of ECE, Thanthai Periyar Government Institute of Technology, Vellore, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, Thanthai Periyar Government Institute of Technology, Vellore,, Tamilnadu, India[2]

ABSTRACT**:** Enhanced secure data transmission is one of the significant aspects in Mobile Ad hoc Networks (MANETs). A local area network is established in order to maintain cooperation among every node, which are responsible in forwarding and receiving the data packets. A proposed mechanism which is so called as ECBDS that effectively detects the malicious nodes that attempt to launch black hole and worm hole attacks. In our scheme, the address of a neighbour node is used as bait destination address to bait malicious nodes to send route reply (RREP) message, and malicious nodes are detected using a reverse tracing technique. The detected malicious nodes are kept in a black hole list. If the packet delivery ratio is less, then the destination node sends an alarm to the source node to trigger black hole detection.

KEYWORDS: Black hole, DSR, Ecbds, RREQ, RREP, Worm hole.

I.INTRODUCTION

Mobile Ad hoc network (MANET) is a collection of mobile nodes in wireless network without any fixed infrastructure. In MANET any user can communicate with other user within a particular range only. Due to the wide spread availability in mobile devices, mobile Ad-hoc networks are widely used in applications such as Disaster Recovery, and military communications by soldiers and so on. MANETs are vulnerable to severe security threats namely black hole and worm hole attacks. They are also easily affected due to the infrastructure less network. One of the most critical problem in MANETs is security vulnerabilities, which is caused due to the mobile nodes which are dynamically changing the network topology in a infrastructure less network. Hence security remains to be a great challenging task in MANETs. The MANETs posses some special features like limited bandwidth, constantly changing network topology, computation power of nodes, battery, lifetime, and unreliable wireless link used for communication between the hosts in the network.

Figure 1 MOBILE AD-HOC NETWORK

II. EXISTING APPROACH

Dynamic source routing consists of two main processes namely route discovery and route maintenance. In route discovery phase, the source node starts to broadcasts a Route Request (RREQ) packet through the entire network. If an intermediate or adjacent node has routing information to destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route.

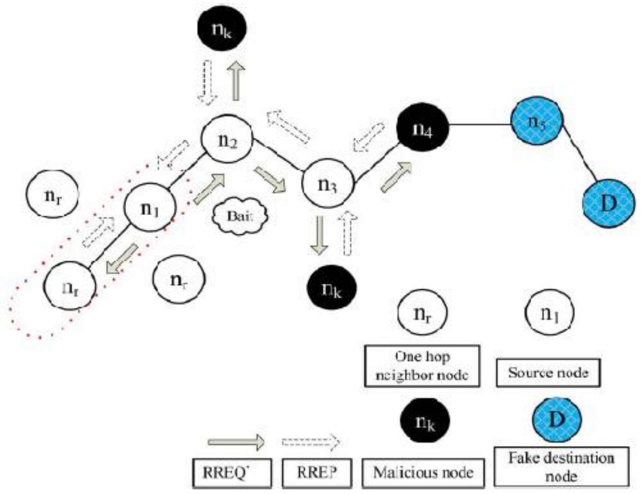


Figure 2 Previous Method System Architecture

DISADVANTAGES OF EXISTING SYSTEM:

- The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole (known as variants of black hole attacks).
- In this regard, the effectiveness of these approaches becomes weak, when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

III PROPOSED APPROACH

The Key Distribution Scheme with shuffling algorithm (KD2SA) is implemented to enhance secure data transmission after the detection of black hole and worm hole attack. Key Distribution Center (KDC) provides a private key '**K**' which is shared between source and the destination. The source generates the key, using number of hops (**H_R**)involved in the route and message sent time (**T_S**) .Using key, data is encrypted at the first level and generates **Ciphertext1**.In the second level**,** Ciphertext1 ,**T_S** and **H_R** are encrypted using **K.** In the second level before encrypting the T_S and $H_{R,}$ they should be shuffled using some **shuffling algorithm.** The Ciphertext2 is sent to the destination and destination makes use of **K** and decrypts the **Ciphertext2.** By using shuffling algorithm, destination obtains values of T_S and $H_{R..}$ By using T_S and $H_{R,}$ destination generates key. The ciphertext1 is decrypted by using key and later the original data is obtained.

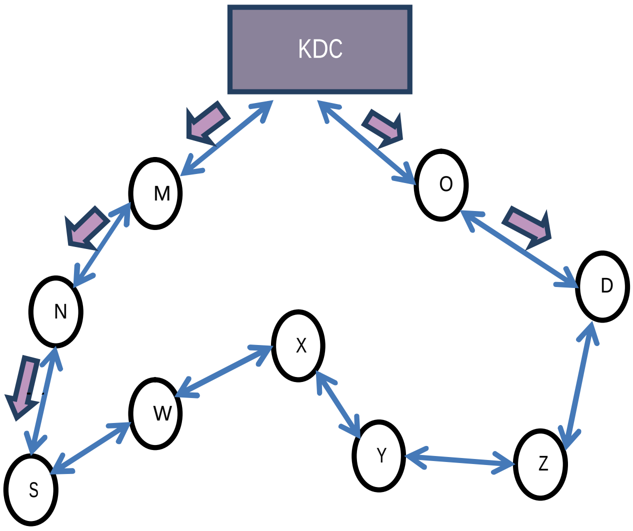
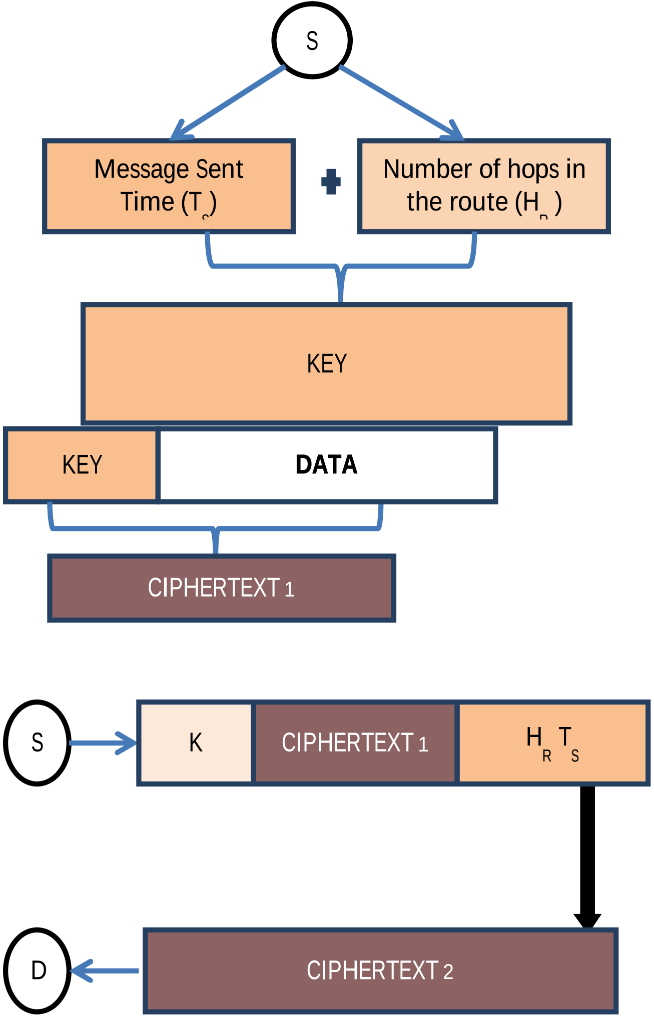


Figure 3 Proposed Architecture



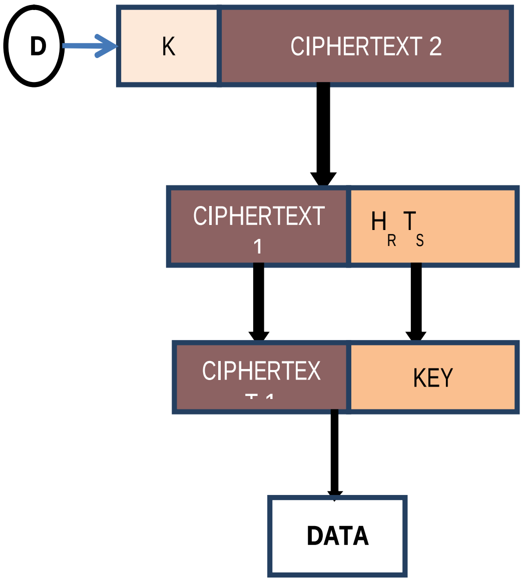


Figure 4 Flow Graph

IV MODULES

- Network Topology
- Dynamic Source Routing Algorithm
- Enhanced Cooperative Bait Detection Scheme
- Performance Metrics

4.1 Network Topology

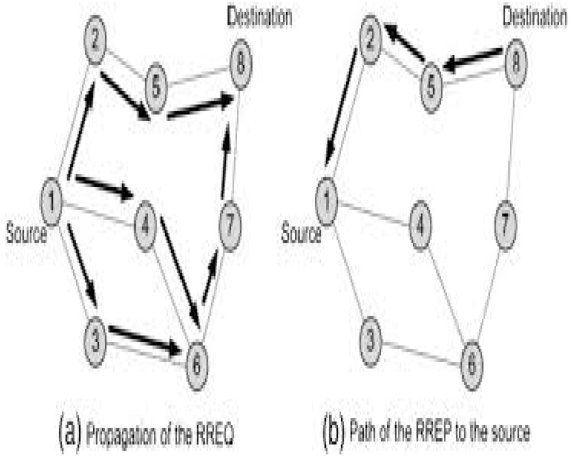
The sensor nodes are randomly distributed in a sensing field. Since MANET is infrastructure less network, the nodes can move independently. In MANET, each node not only works as a host and also acts as a router so that the communication range for all nodes can be found. Every node communicates only within a particular range. If suppose any node is out of range, that node will not communicate with other nodes or simply drops the data packets.

4.2 Dynamic Source Routing Algorithm

In this project, we are using dynamic source routing algorithm for routing. The DSR consists of two main phases namely route discovery and route maintenance. The route discovery consists of RREQ and RREP. The route maintenance involves route error. Each node maintains route cache. When the source node wants to send packets to destination node but does not know route to destination node, the source node initiates rote discovery. The source node broadcasts RREQ throughout the network. If an intermediate node has the route information to the destination node in its cache, it will reply with a RREP to the source node. When a RREQ is forwarded, the node adds its address information in the RREQ packet. When destination receives the RREQ, it can know all the information about intermediate node. Then the destination will reply with RREP to the source node along with the routing information.

4.3 Route Request AND Route Reply

The source node broadcasts route request (RREQ) to all adjacent nodes in the entire network. The route reply (RREP) is received and later the data packets are transmitted from source to destination via intermediate nodes.



(a) Propagation of the RREQ

(b) Path of the RREP to the source

4.4 Black hole Attack

In a black hole attack, malicious node sends a fake RREP to the source node that it has found a route to destination or acts a intermediate node to reach destination. In such case the source node will start to send all of its data packets to the malicious node. As a consequence, the source and destination node will not be able to communicate with each other. As a result, all the packets through the malicious nodes are discarded without forwarding them to destination.

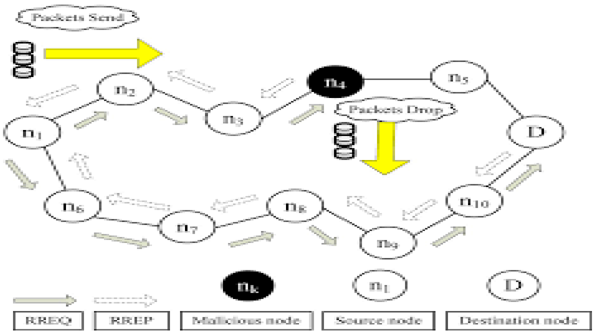


Figure 5 Black hole Attack

4.5 Wormhole Attack

Worm hole nodes fake a route that is shorter than the original one within the network. This can confuse routing mechanisms which rely on the knowledge about distance between nodes. The malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. The tunnel can be established through an out-of band hidden channel (e.g., wired link), packet encapsulation and high powered transmission.

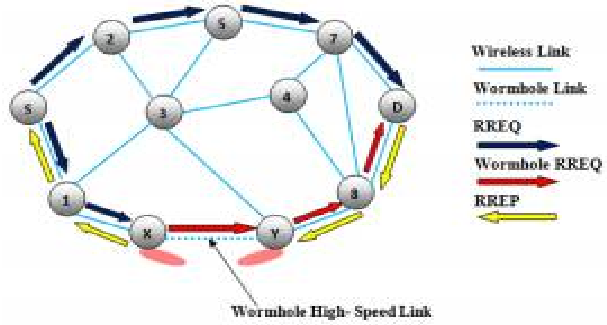


Figure 6 Worm hole Attack

V. ENHANCED COOPERATIVE BAIT DETECTION SCHEME (ECBDS)

We propose a detection scheme uses the bait id and attracts black hole to reply the fake routing information. At first it sends a virtual and random address as its destination address. Proactive detection takes place initially which is used in initial stage and reduces extra routing overhead. When initial process is completed, it becomes reactive detection. After the completion of the process, the packet delivery ratio is checked. If it is less, then destination node sends alarm to the source node which triggers black hole detection.

Performance metrics

In this section, we can evaluate the performance of simulation by using x-graph. We choose the three evaluation metrics:

(i)Packet Delivery Ratio – The ratio of the number of packet received at destination and number of packet sent by the source.

(ii) End-to-End delay – The average time taken for a packet to be transmitted from the source to destination,

(ii) Throughput – The number of data received by the destination without any losses.

VI. RESULTS AND DISCUSSIONS

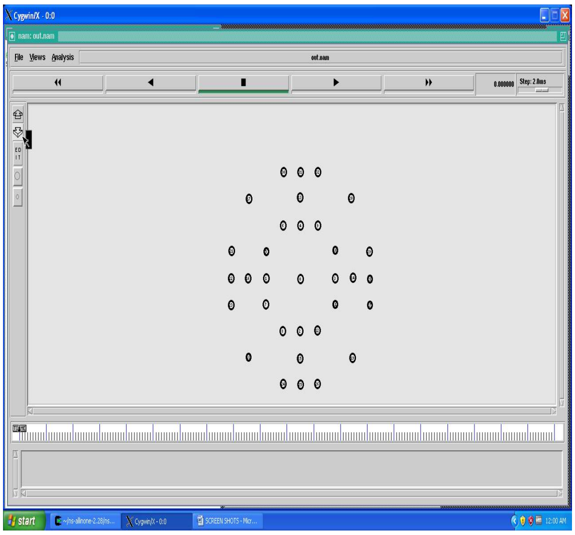
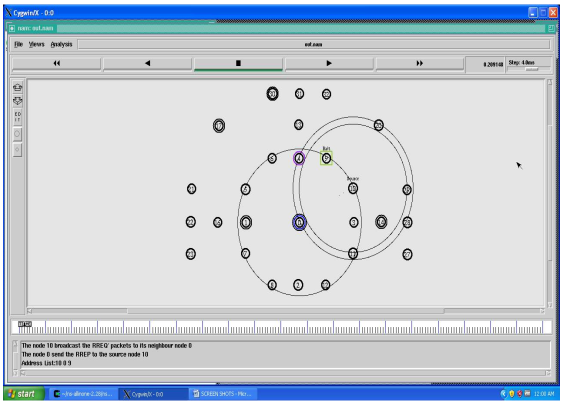


Figure 7 Network Topology

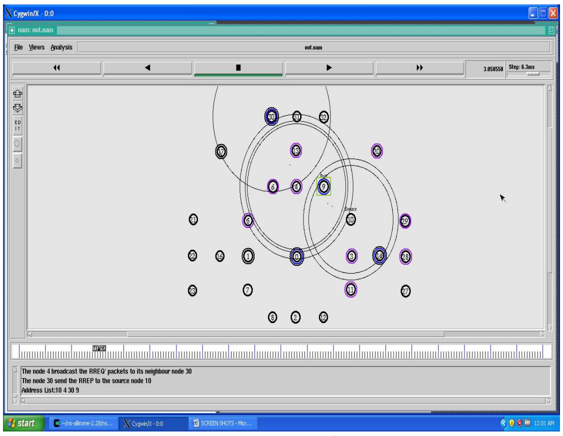
The source and destination nodes are selected for data packet transmission in network.



The node 10 broadcast the RREQ' packets to its neighbour node 0
The node 0 send the RREP to the source node 10
Address List:10 0 9

Figure 8 Packet Transmission

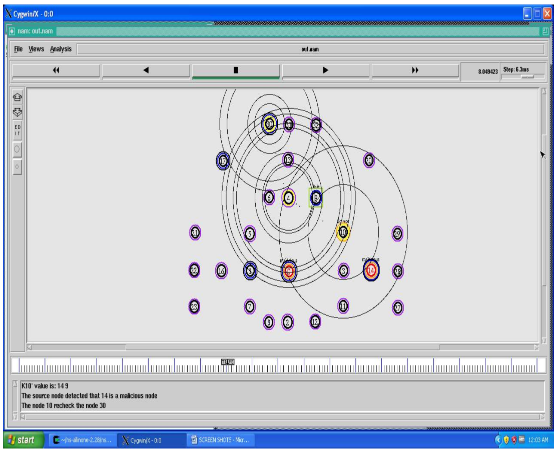
Source node sends packets to destination node via neighboring nodes.



The node 4 broadcast the RREQ' packets to its neighbour node 30
The node 30 send the RREP to the source node 10
Address List:10 4 30 9

Figure 9 Detection of Bait Node

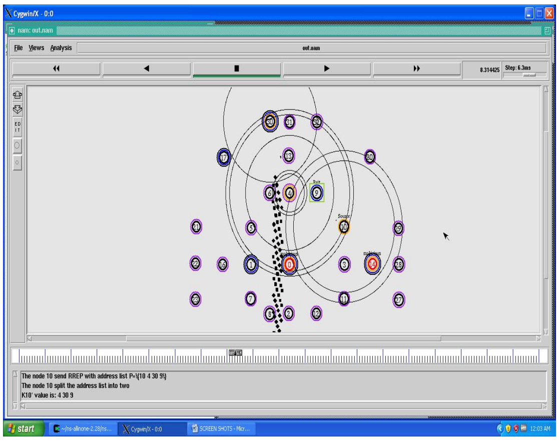
The bait node is detected by the adjacent nodes and the packet transmission may or may not take place through this node.



K10' value is: 14 9
The source node detected that 14 is a malicious node
The node 10 recheck the node 30

Figure 10 Detection of malicious node

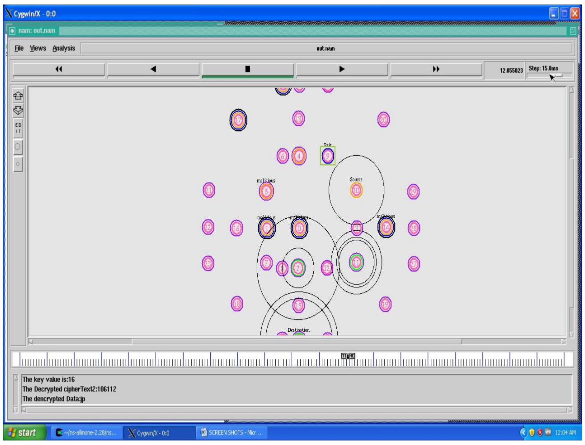
The malicious nodes are detected by the auditor nodes and packet transmission is stopped via these nodes.



The node 10 send RREP with address list P=\{10 4 30 9\}
The node 10 split the address list into two
K10' value is: 4 30 9

Figure 11 Placing malicious nodes in black hole list

The packet delivery ratio is checked and if drop in packet delivery ratio is found, destination node sends alarm to the source which triggers the black hole detection.



The key value is:16
The Decrypted cipherText2:106112
The dencrypted Data:jp

Figure 12 Secured data transmission by KD2SA

The data is transmitted in a secured manner by using key distribution center with shuffling algorithm.

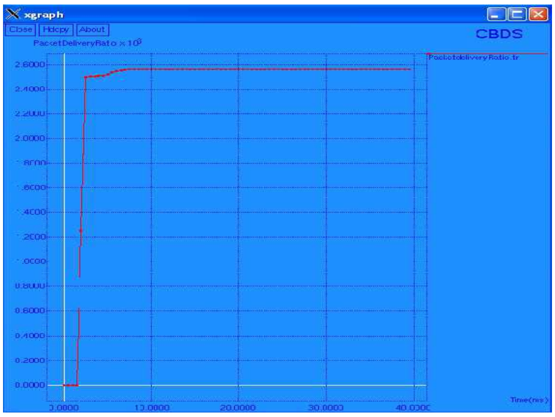


Figure 13 Packet Delivery Ratios.

Packet delivery ratio is the ratio of the number of packet received at destination and number of packet sent by the source. The greater value of packet delivery ratio means the better performance of network.

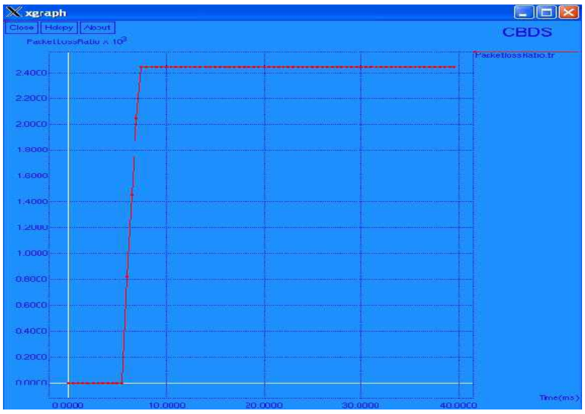


Figure 14 Packet Loss Ratio

The packet loss occurs when one or more packets of data travelling across computer network fail to reach their destination. Packet loss is measured as a percentage of packet lost with respect to packets sent.

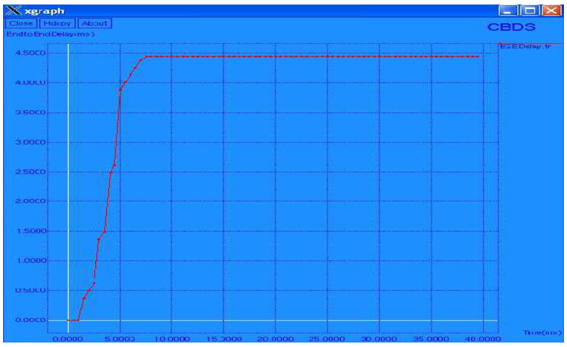


Figure 15 End To End Delay.

End-to-End delay is the average time taken for a packet to be transmitted from source to destination. The lower value of end to end delay means the better performance of network.

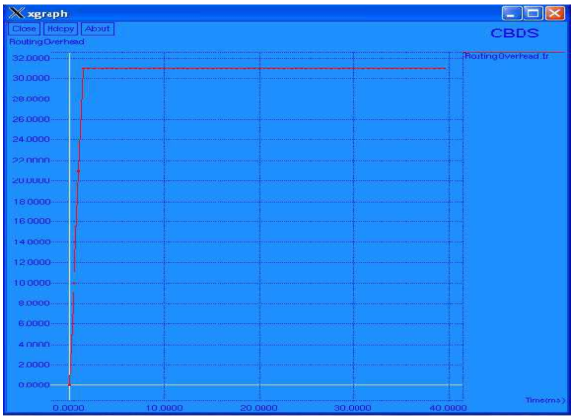


Figure 16 Routing Overhead.

Routing Overhead is the number of routing packets required by the routing protocol to construct and maintain the routes.

VII CONCLUSION AND FUTURE WORK

In this paper we have found a solution to find malicious nodes present in the network. Therefore, the proposed mechanism can be used to detect the flooding black hole and worm hole attacks in MANETs and also identifies secure path from source to destination.
As a future work this method can be extended for (1) detection of various security threats.(2)Study the effects of flooding/rushing attacks.

REFERENCES

[1] Ju Ren, Yaoxue Zhang, Kuan Zhang and Xuemin ”Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks,” IEEE Trans. Wireless Commun., vol. 15, pp. 3718-3731, May 2016.

[2] C. Chang, Y.Wang, and H. Chao, “An efficient Mesh-based core multicast routing protocol on MANETs,” J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[3]P.-C. Tsou, J.-M.Chang, H.-C.Chao, and J.-L. Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,” in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[4] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” Mobile Comput., pp. 153–181, 1996.

[5]S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available:http://www.elook.org/computing/rfc/rfc2501.html

[6] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile-backbone protocol for ad hoc wireless networks,” in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[7] A. Baadache and A. Belmehdi, “Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks,” Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[9] K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[10] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, “An Acknowledgement based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.