International Journal of Technology and Engineering System (IJTES)
Vol 7. No.1 2015 Pp. 69-75
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

AN ENHANCED BAIT APPROACH TO DEFEND AGAINST COLLABORATIVE ATTACKS IN MANETS

[1]R.SOMASUNDARAM, [2]DR.P.SIVAKUMAR AND [3]K.SUMITHRA
[1,3]M.Tech Student., Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.
somu15.diamond@gmail.com.
[2] Associate Professor, Department of Information Technology, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.

ABSTRACT

The dynamic changing topology of Mobile Ad-hoc Network (MANET) makes a node to join and leave the network at any time. The routes between the nodes in the network are established using routing protocols in MANET. The routing protocols are vulnerable to many kinds of security attacks such as blackhole and grayhole attacks. The Black hole attack is a type of attack where a malicious node advertises itself as if it is having the optimal and shortest route to the destination. To resolve these attack issues a mechanism is proposed which is an Enhanced Bait Detection Approach. The proposed scheme embeds the feature of Dynamic Source Routing (DSR) protocol in Ad-hoc On Demand Distance-Vector Routing (AODV) protocol. The scheme comprises of three steps the bait step, Dubious path detection and the Confirmation request and RREP. The bait approach attracts the malicious node to send a reply and in the next step detects the suspected path. The last step involves the destination requesting its neighbor to confirm if the path given is secure. The work is implemented in Network Simulator. Simulation results for performance metric such as Packet Delivery Fraction, Throughput and Overhead are provided.

Index Terms — Blackhole, Bait, DSR, AODV

I. INTRODUCTION

A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes that transmit across a wireless communication medium. MANET has no existing or centralized infrastructure. Each node among the MANETs not only works as a host but also play the role of a router. While receiving data, nodes also need to help other nodes to forward packets, and hence forming a wireless local area network. It is mainly useful in rescue operation and emergency situations such as quick medical assistance, disaster relief services during any major calamity, and military network in battlefields. But MANETs have dynamically changing network topologies, infrastructureless and limited bandwidth and power and hence are vulnerable to different threats. Mobile ad-hoc networks having different types of routing protocols like reactive, hybrid, and proactive protocols type of routing protocols. The design of these routing protocol trusts completely that all nodes would transmit route request or data packets correctly. But they are vulnerable to routing attacks. One of common attack is blackhole attack in which a malicious node can attract all packets by using forged RREP to falsely claim itself as having the fresh and shortest route to the destination and then discard them without forwarding them to the destination. Blackhole attack is a kind of Denial of Service attacks and derives Grayhole attack, a variant of blackhole that selectively discards and forwards data packets when packets go through it. Cooperative blackhole attacks include several malicious nodes cooperating with each other to carry out an attack. This kind of attack results in many detecting mechanisms fail and causes more immense harm to network. The increase of cheaper, small and more powerful devices make MANET a fastest growing network. A mobile ad-hoc network is shown in Fig. 1. Detection mechanisms have been grouped into two broad categories: (i) Proactive approach and (ii) Reactive approach. In Proactive detection schemes nearby nodes are constantly detected or monitored. Reactive detection schemes are those that trigger or activate only when the destination node detects a significant drop in the packet delivery fraction. Mostly this approach uses a threshold based algorithms for continuous maintenance.

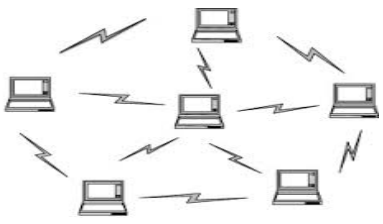


Fig. 1. Mobile Ad-hoc Network

II. OVERVIEW OF DSR AND AODV

A.DSR operation.

DSR is a reactive protocol and therefore doesn't use periodic updates of routing information. It computes the routes whenever needed and then maintains them. The distinguishing feature of Dynamic Source Routing (DSR) is the use of source routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass. The sender lists this route in the packet's header to identify each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination node There are two basic steps of DSR protocol: (i) Route discovery and (ii) Route maintenance. Every node in the network maintains a cache to store latest discovered paths. Before a node sends a packet, it first checks the cache whether there is an entry for that path. If it exists then this path is used to send the packet and attaches its source address on the packet. The source node broadcasts a route request packet to all its neighbors querying for a route to the destination only if there is no existing entry or if the entry has expired. Until the route to destination is discovered, the sender node waits for the route reply. When the route request packet arrives at other nodes, they check if they have a route to the destination. Only if they have, they send back a route reply packet to the destination else they broadcast the same route request packet to its neighbors.

Once the route to destination is discovered, the data packets to be send by the source node are sent using the discovered route. The entry is inserted in the cache for use in future. Also the node keeps the freshness information of the entry to recognize whether the cache is fresh or not. If any intermediate node receives a data packet, it first checks whether the packet is sent to itself. If it is the destination, it accepts the packet else it forwards the packet to the destination using the route attached on the packet.

B. Merits and Demerits of DSR

DSR have very low overhead on route maintenance. This is because routes are maintained only between nodes who want to communicate. Caching of routes further reduces route discovery overhead. Many routes to the destination are yielded by a single route discovery due to intermediate nodes reply from local caches. These are the various advantages of DSR.

The disadvantage is that the packet header size grows in length due to route caching. Due to flooding of route requests packets, it reaches all nodes in the network. Hence collisions may occur between route requests propagated by neighboring nodes. Nodes replying using their cache increases contention.

C. AODV operatio

AODV (Ad-hoc On-Demand Distance Vector) routing protocol is a protocol where nodes need not maintain routes to destination that are not on active path. Route messages like Route Request (RREQ), Route Reply (RREP) and Route Error (RRER) are used to discover routes and maintain links between nodes. AODV uses a destination sequence number for each route created by destination node for any request to the nodes. A route having the maximum sequence number is selected for transmission of packets. To find a new route to destination the source node broadcasts Route Request packet in the network till it reaches the destination. The destination replies with the Route Reply packet to source. The nodes on active path communicate with each other by sending hello packets periodically to its one hop neighbor. If there is no reply from nodes then it deletes the node from its list and sends Route Error to all the members in the active route.

D. Merits and Demerits of AODV

The main advantage of this protocol is having routes established on demand and that destination sequence numbers are used to find the latest path to the destination. Also the delay in connection setup is low.

However intermediate nodes can lead to inconsistent routes due to old source sequence number and the intermediate nodes have a higher but not the newest destination sequence number, thereby leading to stale entries. Heavy control overhead is caused by response of multiple Route Reply packets for a single Route Request packet. Another major disadvantage of AODV is high consumption of bandwidth due to periodic broadcasting of beacon.

III. RELATED WORK

A method was introduced in [6] to find the secured routes and prevent the blackhole nodes (malicious node) in the MANET by checking whether there is much large difference between the sequence number of source node or intermediate node who has sent back RREP or not. The first route reply will be from the malicious node with high destination sequence number. It is stored as the first entry in the RR-Table. The first destination sequence number is compared with the source node sequence number. If there is a large difference between them, then that node is the malicious node. This malicious node's entry is then removed that entry from the RR-Table. But this approach has no detection scheme after route discovery process.

In [10] the working of the source node in original AODV protocol was modified by using an additional function Pre_ReceiveReply (Packet P). In addition to this a new table Cmg_RREP_Tab, a variable Mali_node and a timer MOS_WAIT_TIME are added to the data structures. The newly created table, Cmg_RREP_Tab stores all the RREPs until the time, MOS_WAIT_TIME. By heuristics, MOS_WAIT_TIME is initialized to be half the value of RREP_WAIT_TIME. It is the time for which source node waits for RREP control messages before regenerating RREQ. Then all the stored RREPs from Cmg_RREP_Tab table are analyzed by the source node. The RREP having a very high destination sequence number is removed. The node which sent this RREP is suspected to be the

malicious node. This technique was effective in detecting single blackhole node.

A new scheme is proposed in [11] called DPRAODV (Detection, Prevention and Reactive AODV). In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If the RREP_seq_no is higher than the one in routing table then only the RREP packet is accpeted. But DPRAODV does an extra check to find whether the RREP_seq_no is higher than the threshold value which is dynamically updated. If the value of RREP_seq_no is found to be higher than the threshold value, then this node is suspected to be malicious and it adds the node to the black list. Due to detection of an anomaly, it sends a new control packet, ALARM to its neighbors. The computation of threshold value is done by finding the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet.

The survey of various techniques used to detect and prevent blackhole attacks are detailed in [5]. Defects in each method have also been listed. Some of the single blackhole attack detection schemes are Neighborhood based and Routing Recovery, Redundant Route and Unique Sequence Number Scheme, Time-based Threshold Detection Scheme, Random Two hop ACK and Bayesian Detection Scheme, DPRAODV, Next Hop Information Scheme and IDS based on ABM. Some of the Collaborative Blackhole attack schemes are DRI (Data Routing Information) and cross Checking scheme, Distributed Cooperative Mechanism (DCM), MAC and Hash based PRF Scheme and Bait DSR (BDSR). This literature have briefed the various schemes to prevent blackhole attacks and compared the results. The improved AODV using the function Pre_ReceiveReply had no proposal for preventing collaborative blackhole attacks. The DPRAODV method failed to detect cooperative blackhole attacks in MANETs.

IV. THE PROPOSED SCHEME

The enhanced bait approach enhanced proactive scheme. It embeds the feature of DSR in AODV like the caching of path information in RREP. It consists of three steps.

- Bait step
- Dubious path detection
- Confirmation Request and RREP

All the nodes cooperate with each other using HELLO packets before the start of the bait step. The operation of the proposed scheme is shown in Fig. 4.

A. Bait Step

The aim of the bait phase is to entice a malicious node to send a fake (forged) RREP (RouteRequest) to the bait RREQ'. The malicious blackhole node advertises itself as having the shortest and optimal path to the destination node. In order to generate bait RREQ' the source node randomly selects an adjacent node, say np, within its one-hop neighborhood nodes and cooperates with this node and takes its address as the destination address of the bait RREQ' packet. The source node broadcasts the fake RREQ' (bait RREQ') containing the address of one hop node np as the destination address. If any node sends a RREP (RouteReply) for this bait RREQ' it indicates that the malicious node exists in the network. Even if there many blackhole nodes, this technique works with ease in detecting the malicious node. The blackhole list lists the nodes which reply to the bait RREQ'. The source nodes ignore the packets received from such malicious nodes in future.

B. Dubious path detection

The identity of malicious nodes is found in the dubious path detection step through the route reply sent for the bait RREQ' message. If a malicious node has received the RREQ, it will reply with a forged RREP. Dubious path detection is conducted for nodes receiving the RREP, with an aim to deduce the suspected path information in the network which may have a malicious node. This step makes uses of DSR property. The enhanced bait approach is able to detect more than one malicious node, when these nodes send reply RREPs. Consider for example, nn, a malicious blackhole node replies with a false (forged) RREP. An address list A = {n1...nh...nn...np} is stored in the RREP. The node n1 is the source node. When a node nh receives the RREP, it obtains the address list Th = {n1...nh}. Th is obtained by separating the list A by the destination address n1 of the RREP where Th represents the path information from source node n1 to destination node nh. The differences between the address list A = {n1…n2...nh...nn...np} stored in the RREP and Th = {n1…n2...nh} is determined by node nh. Hence we get

$$T' = A - Th = \{nh+1...nn...np\} \quad (1)$$

The T' is stored in RREP packet. The RREP and the address list T'h of the nodes that received the RREP are received by the source node. To ensure that T' does not come from a malicious node, if node nh received the RREP, it will compare: (i) The node address of source in RREP; (ii)The next hop of nh in the list A and (iii) One hop of node nh. If (i) do not match with (ii) and (iii), then the received Th can do a forward back. But if there is a match then nh should forward back the T' which it produced. The source node then performs the intersection of T'h to obtain the dubious path S.

$$S = T'1 \cap T'2 \cap \ldots \cap T'h \quad (2)$$

In the Fig. 2 the source node S broadcasts the RREQ throughout the network. A source route request packet carries the source sequence number and destination sequence number, the source identifier (SrcID), the destination identifier (DestID), broadcast identifier (BcastID) and the time to live (TTL). The freshness of the route is indicated by the Destination sequence number (DestSeqNum). The duplicate copies of the route request packet are discarded by seeing the BcastID-SrcID pair.

The RREQ also includes an array to store the traversed path in RREQ just like how DSR carries the path information. The sequence number at intermediate node with the destination sequence number in the RREQ packet to check the validity of a route at the intermediate node.

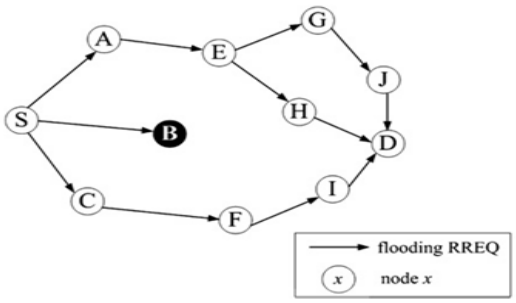


Fig. 2. RREQ flooding

C. Confirmation Request and RREP

The source node now sends the original RREQ addressed to some destination in network. After the destination receives the RREQ, it broadcasts a confirmation message in form of hello packets to its one-hop neighbor. This packet asks its neighbors if the path sent to it has any malicious node. The neighbor nodes check its blackhole list and if there was no update of malicious node on the path it doesn't reply to destination. The neighbor node responds to destination only if the chosen path has a malicious node. This is done to check if given path contains malicious node. The destination then chooses the secure path with the latest destination number and forwards the RREP along the path.

The malicious node, B as well as the destination node, D replies to the RREQ with an RREP as shown in Fig. 3.

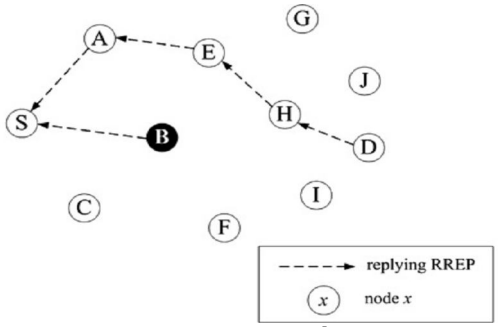
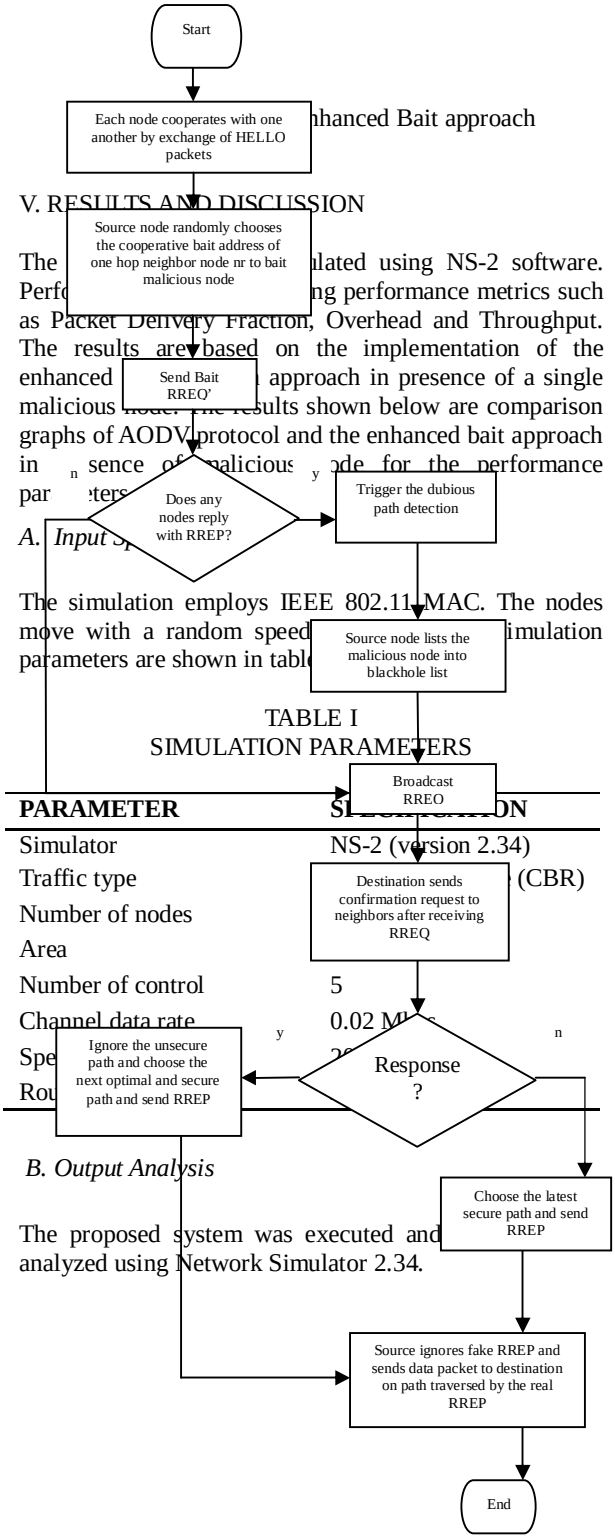


Fig. 3. RREP reply

A node stores the receiving RREP packet information from the previous node from which the packet was received so that the data packet can be forwarded to this node as the next hop towards the destination. The source node after it gets the RREP forwards the data along the path traversed by RREP. The source node can distinguish the real RREP and fake RREP and ignores the fake RREP. Source node forwards the data packet only along the secure path and data forwarding is done as in normal AODV operation.



V. RESULTS AND DISCUSSION

The ulated using NS-2 software. Perf ng performance metrics such as Packet Delivery Fraction, Overhead and Throughput. The results are based on the implementation of the enhanced approach in presence of a single malicious node. The results shown below are comparison graphs of AODV protocol and the enhanced bait approach in sence of malicious ode for the performance par eters.

A. Input S

The simulation employs IEEE 802.11 MAC. The nodes move with a random speed imulation parameters are shown in tabl

TABLE I
SIMULATION PARAMETERS

PARAMETER	SPECIFICATION
Simulator	NS-2 (version 2.34)
Traffic type	(CBR)
Number of nodes	
Area	
Number of control	5
Channel data rate	0.02 M
Spe	
Rou	

B. Output Analysis

The proposed system was executed and analyzed using Network Simulator 2.34.

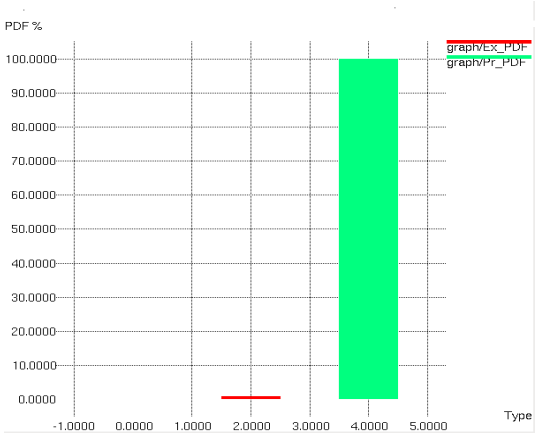


Fig. 5. PDF comparison graph

Fig. 5 shows the Packet Delivery Fraction (PDF) comparison of the existing AODV with the proposed system.

$$PDF = \frac{\text{Number of packets received by the destination node (3)}}{\text{Number of packets sent by source node}}$$

The PDF is calculated using (3). The number of packets sent is 54 and due to presence of malicious node in existing AODV the received packet is nil as all packets are received by the blackhole node and dropped. The packet loss is 54 and hence PDF is 0% or nearly zero. But in proposed scheme the blackhole attack is prevented and hence there is no packet loss. The PDF is 100% as all the packets are delivered to the destination.

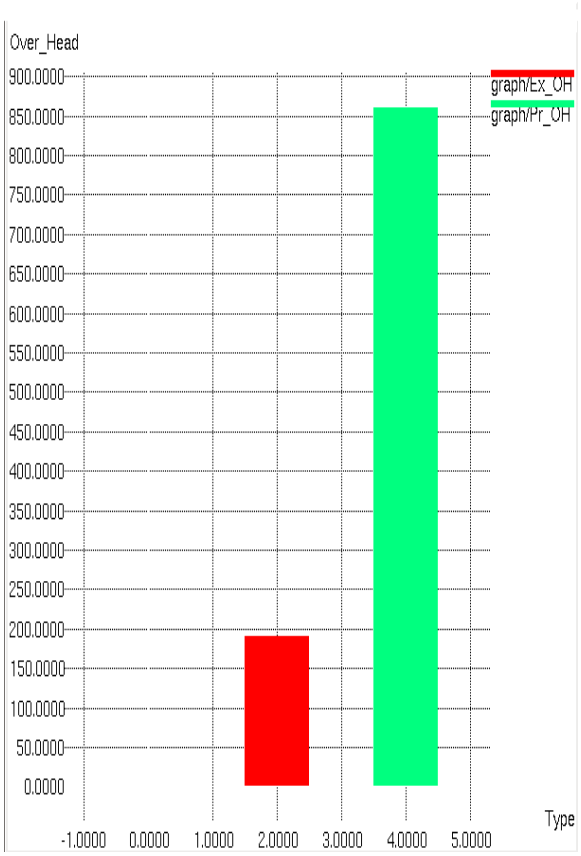


Fig. 6. Overhead comparison graph

Fig. 6 shows the routing overhead (no of control packets) of existing and proposed system. In the proposed system the cooperation of nodes and the bait RREQ' creates high overhead. The existing AODV has overhead of 190 Kbps and the proposed system has high overhead of 861. Overhead is the ratio the amount of control packets transmissions to the amount of data transmission.

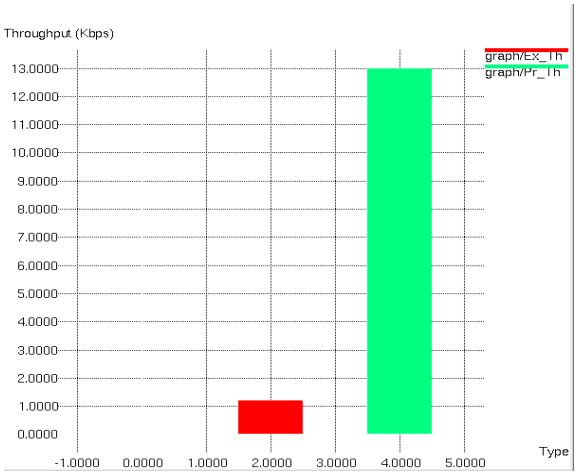


Fig. 7. Throughput comparison

Fig. 7 shows the Throughput comparison of the existing AODV and proposed scheme. The throughput is the number of bits sent per second. The existing AODV has a throughput of 1200 bits per second (1.2 Kbps) and the proposed system has a throughput of 13000 bits per second (13 Kbps) higher than the existing AODV. This is because of detection and prevention of blackholes. The proposed scheme also has some more delay compared to existing AODV due to bait and confirmation steps

VI. CONCLUSION AND FUTURE WORK

The enhanced bait approach is proposed to prevent to detect and prevent blackhole attacks. It combines the features of AODV and DSR to identify blackhole node and prevents packet loss due to blackhole attack. The proposed system was simulated using Network Simulator and results are analyzed. From the results it is observed that the proposed system performs well in terms of PDF and throughput but has a high overhead with them due to additional control packets. The proposed scheme is a proactive detection approach. For future work inclusion of a better reactive detection scheme can improve efficiency at real time by monitoring continuously. Also detection and prevention from other attacks such as wormhole attacks can be done with some modifications to the proposed code. This increases the versatility to detect and prevent two to three types of attack.

REFERENCES

[1] Barleen Shinh and Manwinder Singh, "Detection and Isolation of Multiple Black Hole Attack Using Modified DSR," International journal of Emerging Trends in Science and Technology,vol. 1,Issue 4, pp. 540-545, June 2014.

[2] Chander Diwaker and Sunita Choudhary , "Detection Of Blackhole Attack In Dsr Based Manet," International Journal of Software and Web Sciences (IJSWS), vol. 4,pp. 130-133,March-May 2013.

[3] Chun-Hsin Wang and Yang-Tang Li, "Active Black Holes Detection in Ad-Hoc Wireless Networks," IEEE, pp. 94-99, 2013.

[4] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089-1098, March 2013.

[5] Fan-Hsun Tseng,li-Der Chou and Han_chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric and Information Sciences,1:4, 2011.

[6] Lalit Himral, Vishal Vig and Nagesh Chand , "Preventing Aodv Routing protocol from Black Hole Attack," International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 5, pp. 3927-3932, May 2011.

[7] M. Mohanapriya and Ilango Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," Computers and Electrical Engineering, pp. 530–538, 2014.

[8] G.S. Mamatha and S.C. Sharma, "A Highly Secured Approach against Attacks in MANETS," International Journal of Computer Theory and Engineering, vol. 2, no. 5, pp. 815-819, October 2010.

[9] Ming-Yang Su, "Prevention of selective black hole attacks on mobile adhoc networks through intrusion detection system," Computer communications, pp. 107-117, 2011.

[10] Nital Mistry, Devesh C Jinwala and Mukesh Zaveri "Improving AODV Protocol against Blackhole Attacks," in Proc. 2010 International Multiconference of Engineers and Computer Scientists (IMECS), Hong Kong, vol. 2.

[11] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dyanamic Learning System against Blackhole Attack In AODV based Manet," IJCSI International Journal of Computer Science Issues, vol. 2, pp. 54-59, 2009.

[12] Po-Chun 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, pp. 1–5, 2011.

[13] Prachee N. Patil and Ashish T. Bhole, "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching," IEEE Wireless and Optical Communications Networks (WOCN)*, pp. 1-6, 2013.*

[14] K. Selvavinayaki, K.K. Shyam Shankar and E. Karthikeyan, "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs," International Journal of Computer Applications, vol. 7, No.11,pp. 15-19, 2010.

[15] Seryvuth Tan and Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attackson AODV-based MANETs," IEEE International Conference on High Performance Computing and Communication and IEEE International Conference on Embedded and ubiquitous Computing, pp. 1159-1164, 2013.

[16] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges," IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 658 – 672, 2011.

[17] Vikas Solomon Abel, "Survey of Current and Future Trends in Security in Wireless Networks,"

International Journal of Scientific & Engineering Research, vol. 2, Issue 4, pp. 1- 6, April 2011.

[18] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu, "Risk-Aware Mitigation for MANET Routing Attacks," IEEE Transactions on Dependable And Secure Computing, vol. 9, no. 2,pp. 250-260, March/April 2012.