ECBDS: Enhanced Cooperative Bait Detection Scheme for Preventing Collaborative Attacks in MANETS

Abdul Jawad PP[1], Bismin Chacko[2]

[1]Final Year Student, M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

Abstract: ***Providing secure communication is one of important aspects in Mobile Ad hoc Networks (MANETs). Routing between Source and destination must be secure. Routing protocols helps to transfer the packets to destination. Routing Protocols are vulnerable to collaborative black hole attacks. When malicious nodes work together, to drop the packets called collaborative attacks, Blackhole attacks completely drops the packets in MANETs and also advertise that, it has minimum shortest path to destination. We propose a mechanism, Enhanced Cooperative Bait Detection Scheme (ECBDS) for preventing Collaborative blackhole attacks in MANETs. In this mechanism, integrates features of Dynamic Source Routing (DSR) and 2ACK protocols. ECBDS scheme merges the proactive and reactive defense architecture and ensure secure data transmission using Key Distribution Scheme shuffling Algorithm . In the initial stage it uses a proactive architecture, i.e. uses a Bait id concept for the detection of malicious nodes present in the network. Upon the completion of initial stage it switches to reactive defense strategy. The scheme comprises of three steps, the bait step, suspected path detection and the Confirmation Request. 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. To secure data transmission we use key distribution shuffling algorithm scheme and encryption using Key generated by KDC.The work is implemented in Network Simulator. Comparing performance of ECBDS with DSR and 2ACK. ECBDS simulation result shows increased packet delivery ratio, throughput and reduced End to End Delay ratio.***

Keywords: Black hole, Bait, DSR, 2ACK, MANET

1. Introduction

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes in wireless network without any fixed infrastructures. In this network, intermediate nodes cooperate and act as a router and send messages from one node to another. MANETs is rapidly deployable and it also highly adaptive in nature. Nodes have high mobility and communication is done via shared wireless network. MANETs are widely used in applications such as military communication by soldiers, Emergency rescue service, Disaster Recovery, etc. In MANETs have some particular characteristics such as unreliable wireless links used for communication between many host, limited bandwidth, constantly changing the network topology, enumeration power and low battery power etc.

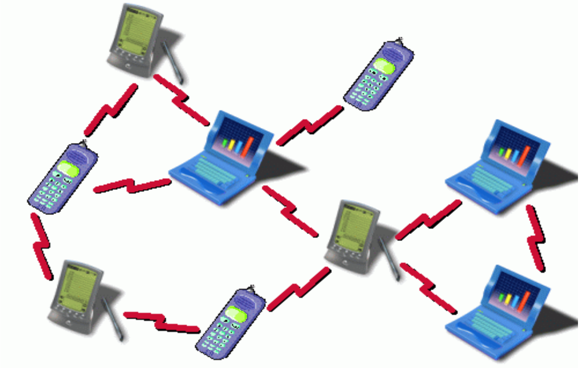


Figure 1: MANETs

In Mobile Ad hoc Networks there is no infrastructure support as in case with wireless networks. Since a destination node might be instead of the range in a source node sending packets; a routing process is at all times needed to find a path so as to forward the packets suitably among the source node and the destination node. In a cell, a base station can reach all mobile nodes without routing by means of broadcast in generic wireless networks. In the process of ad-hoc networks, each node should be able to forward data to the other nodes

The lack of any infrastructure, mobile nodes are dynamically changing the network topology in infrastructure less network makes MANET more vulnerable to various types of routing attacks than a typical wireless network. The attacker would perform different types of attacks such as Black hole, Collaborative Blackhole and Gra hole attack.

1.1 Blackhole Attack

In a blackhole attack, a malicious node sends a fake RREP packet to the source node that has initiated a route discovery process and in order to show itself as a destination node or an intermediate node to the actual destination node to the route. In such a case the source node would send all of its data packets to the malicious node and the malicious node then intercepting the packets. A result of source node and destination node will not be able to communicate with each other. Also a malicious node does not need to check its routing table when sending a false message; its response is more likely to diffuse the source node first. This makes the source node consider that the route discovery process is complete and that is ignore all other reply messages and begin to send data packets. As a result of this process, all the packets through the malicious node are discard without forwarding them to the destination.

1.2 Collaborative Blackhole Attack

The malicious node could be said to form a black hole in the network. In sometimes these malicious nodes are cooperate with each other with the same aim of dropping packets these are known as collaborative Black Hole nodes and the attack is known as Collaborative Black Hole attack.

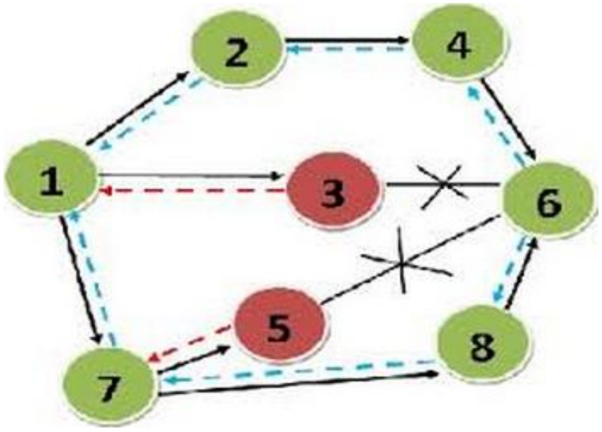


Figure 2: Collaborative Blackhole Attack

1.3 Gray Hole Attack

Gray hole attack is a variation of black hole attack, in which the malicious node‟s are more difficult to detect. The gray hole nodes can perform the attack in three different ways:

a) The malicious node may drop packets from certain nodes while forwards all other packets to the network.

b) A node may behave maliciously for a certain time and dropping packets selectively.

c) The malicious node may drop packets from specific nodes for precise time only, but later on it behaves as a normal node. Since, due to these characteristics, the detection of gray hole attacks is very hard. A gray hole attack can disturb the route discovery process and degrade the network‟s performance.

2. DSR and 2ACK Protocols

2.1 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.

2.2 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.

2.3 2ACK operation

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. 2ACK 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.

2.4 Merits and Demerits of 2ACK

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.

3. Related Works

A number of researches are being carried for enhancing the security in Manet. Since there is no particular line of defense, security for manet is still a major concern for man. Some of the researches for the detection of blackhole attack are given. Kozma, and L.Lazos, "REAct: resource-efficient for node misbehavior in ad hoc networks based on random audits," [9] Based on Audit Procedure. When destination node detects a heavy packet drop, it triggers the source node to initiate the audit procedure. Source node chooses an audit node and it generates behavioral proof. Similarly source node prepares it behavioral proof .On the basis of comparison of results malicious nodes are detected. Drawback was that it is a reactive approach .

Only if there is a drop in packet delivery ratio, the mechanism is triggered. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," [8] Introduced the concept of route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack in AODV. The intermediate node along with RREPs sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node checks in its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. It was dependent on the intermediate nodes reply. Also it was able to detect only single black hole.W. Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," [10] Introduced the approach of hash based function in REAct system. Enabled the data traffic and forward path detail available in behavioral proof. Upon drop in the packet delivery ratio initiates the blackhole detection.

Based on the reactive detection. Latha Tamilselvan and Dr. V Sankaranarayanan," Prevention of Co-operative Black Hole Attack in MANET"[11] designed an approach for detection of co-operative black hole attack, based on the Fidelity table where presence of 0 indicates a malicious node. But it failed for the case of DSR. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol" [6] proposed a simple scheme which depends on the details of intrusion detection from local nodes rather than from the source node. This scheme is used only for the case of AODV as it has the advantage of sequence number.

4. Proposed System

The DSR based secure routing protocol that we are using detects and avoids the black hole attack. ECBDS (Enhanced Bait detection scheme) uses the concept of sending bait id and attracts black hole to reply the fake routing information. Initially it sends a virtual and random address as its destination address. Proactive detection is used initially. In case presence of any malicious node is detected, it is included in the black hole list. We use the proactive detection only in our initial stage. Thereby reducing the routing extra overhead. As soon as the initial stage is over, it becomes reactive detection. Normal packet transmission takes place. Upon the completion of the process it checks the packet delivery ratio. If drop in packet delivery ratio is found, destination node sends alarm to the source which triggers the black hole detection.

Our mechanism merges the advantage of proactive detection in the initial stage followed by superiority of the reactive detection. In ECBDS scheme the packet format of the RREP and RREQ is modified. In case of DSR routing, the source will have all the information about the intermediate nodes participating in its mechanism. Upon the reception of the RREP, it will know details of the nodes participating in packet transmission but it will not know exactly which the malicious node is. The packet format of RREP is modified such that Reserved field is used as Record address. The record address enables to trace the malicious node. In addition it has RREQ‟ packet which has a virtual and non-existent address as its target address. Route discovery is initiated with the source sending RREQ‟ to all the nearby nodes. The target address of the RREQ‟ is a fake id i.e. a virtual non-existing random id is given .When a malicious node receives RREQ‟, it replies itself as the shortest path to the destination. Upon the reception of the RREP, from the record address field, the source will know which the malicious node is and removes it from its network, in its initial stage.

Thus the malicious node is detected and is recorded in the blackhole list. Thus the proactive detection detects the presence of blackhole. Also all the nodes are made aware of the blackhole. The proactive detection makes use of the record address and the false id to perform the detection of the malicious node. Upon detection of the malicious node it is removed from the network by triggering alarm to all the nodes in the network about the malicious node. Thus future responses from the malicious nodes are discarded. After the initial proactive stage, it becomes reactive detection. Source sends the route RREQ to the nearby nodes. The intermediate node sees to the target address. If it is the shortest path to the destination it adds its address to the field and forwards the packet to the destination. In case it has already received the packet it just discards the packet. If it is the target address it sends RREP to the source and normal packet transmission starts. Upon the completion of the process, the destination checks the packet delivery ratio. ECBDS scheme uses the advantage of both the proactive and the reactive detection. In the initial stage it reduces the chance of malicious node. In later stage it becomes reactive detection thereby reducing the overhead.

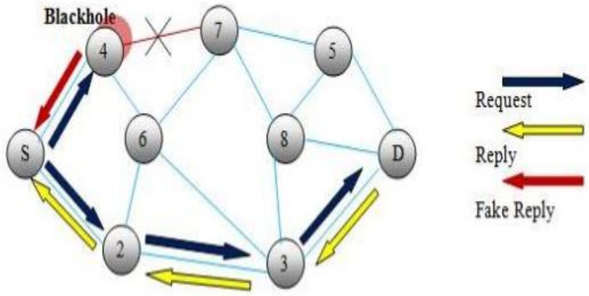
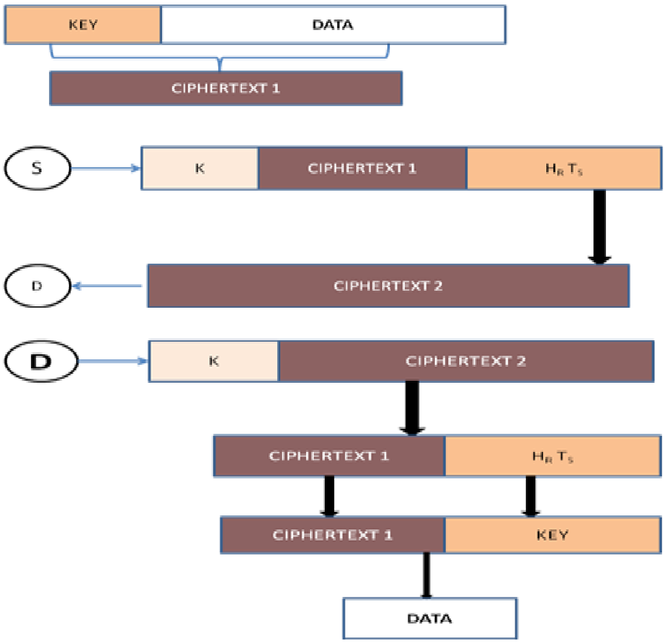


Figure 3: Operation of ECBDS

In case of Co-operative black hole attack, number of malicious node cooperate together and work as a network. This eases the task of detection. When a single malicious node is detected, based on the details of its next hop, we can easily find the remaining malicious nodes present within the network. This scheme performance clearly depicts that it has a greater packet delivery ratio as well as high network throughput and it has reduced routing overhead ratio.

4.1 Secure Data Transmission

To make the data transmission secure after the detection of black hole attack. The Key Distribution Center (KDC) provides key „**K**“ which is shared between source and the destination .Source generates the key **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 ,The destination makes use of **K** and decrypt the **Ciphertext2** by making use of shuffling algorithm, destination obtains values of **T_S** and **H_R** .Using **T_S** and **$H_{R,}$** destination generates **KEY** using **KEY**, **Ciphertext1** is decrypted



5. Simulation Results

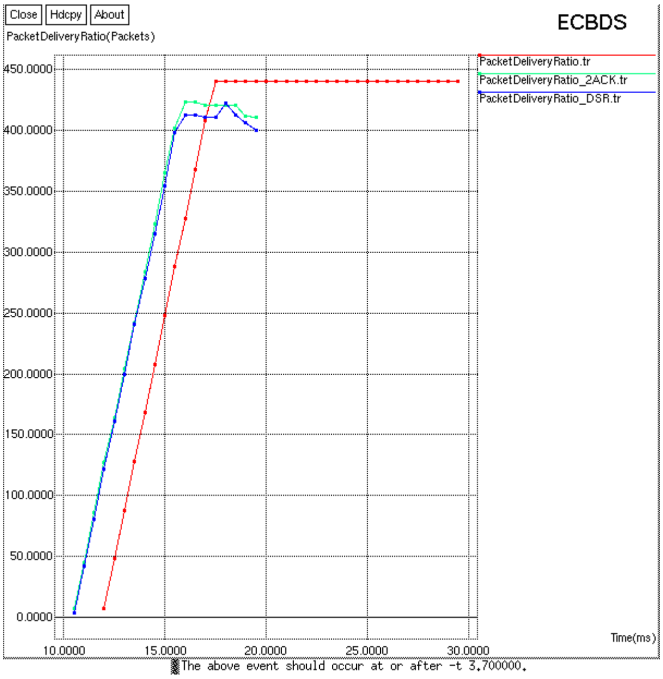
The proposed work is simulated using NS-2 software. Performance is evaluated using performance metrics such as Packet Delivery Ratio, Routing Overhead and Throughput. The results are based on the implementation of the Enhanced Bait Detection Scheme. The results shown below are comparison graphs of 2ACK, DSR protocol and the ECBDS in presence of malicious node for the performance parameters.

5.1 Input Specifications

The simulation employs IEEE 802.11 MAC. The nodes move with a random speed of 20 m/s. The simulation parameters are shown in table below.

Output Analysis

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



```
The above event should occur at or after -t 3.700000.
```

Figure 5: Packet Delivery Ratio

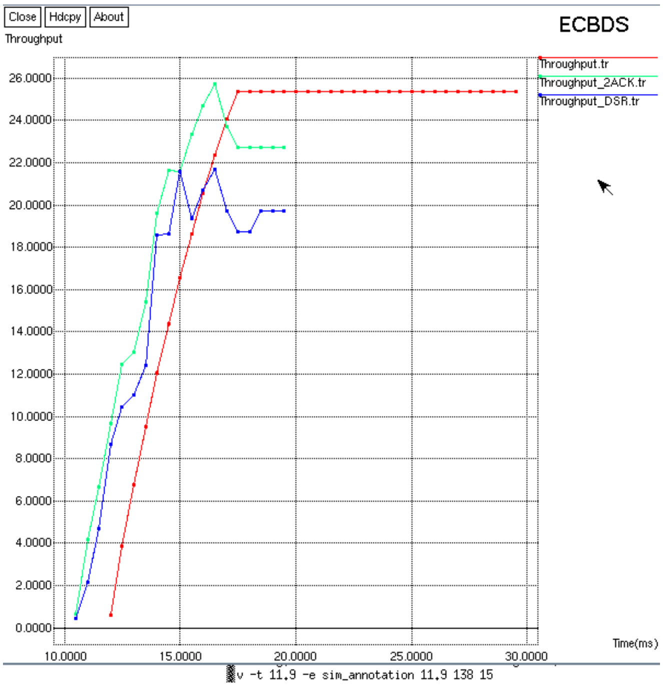
Fig. 5 shows the Packet Delivery Ratio (PDF) comparison of the existing 2ACK and DSR with the proposed system.

PDF = Number of packets received by the destination node to Number of packets sent by source node

The PDR of ECBDS is better than 2ACK and DSR protocols.

Fig. 6 shows the Throughput comparison of the existing 2ACK, DSR with the proposed system.

The Throughput of ECBDS is better than 2ACK and DSR protocols.



```
v -t 11.9 -e sim_annotation 11.9 138 15
```

Figure 6: Throughput

Fig. 7 shows the End to End Delay comparison of the existing 2ACK, DSR with the proposed system.
The End to End Delay of ECBDS is better than 2ACK and DSR protocols.

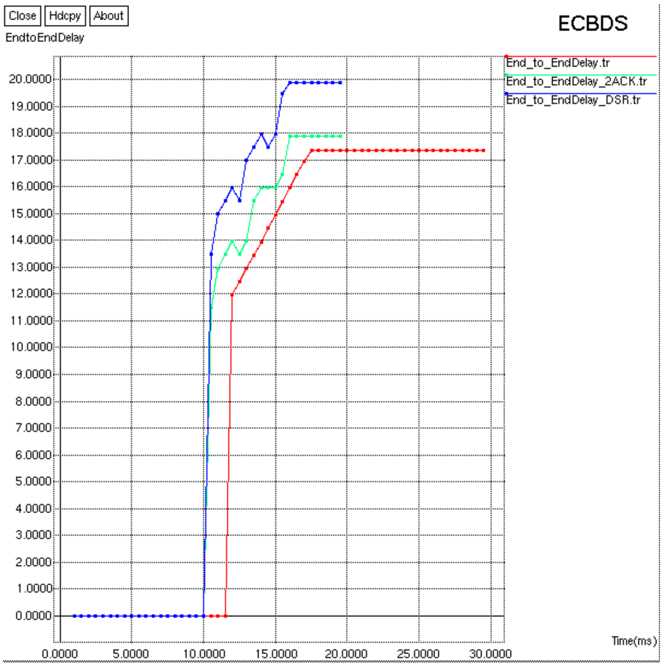
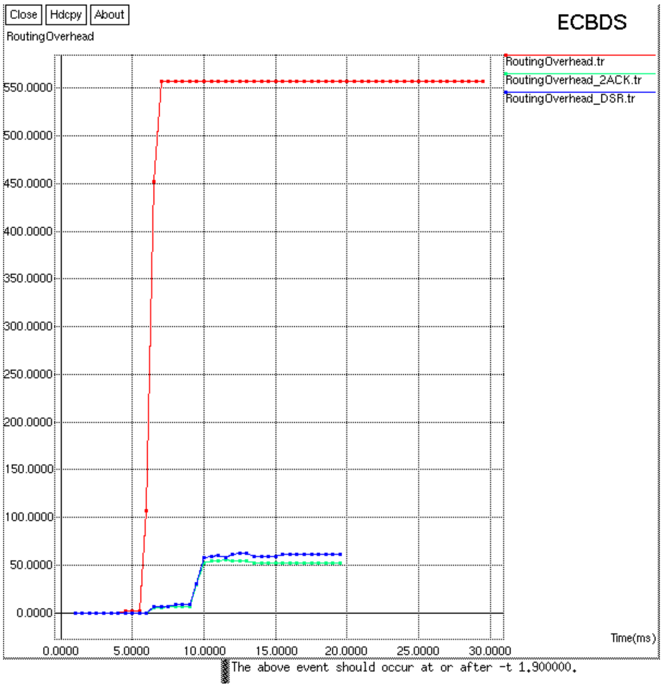


Figure 7: End to End Delay

Fig. 8 shows the Routing Overhead comparison of the existing 2ACK, DSR with the proposed system.

The Routing Overhead of ECBDS is higher than 2ACK and DSR protocols. Because of encryption process & shuffling algorithm in ECBDS.



```
The above event should occur at or after -t 1.900000.
```

Figure 8: Routing Overhead

6. Conclusion and Future Work

The ECBDS detects and avoids the black hole attack in MANETS. It uses the proactive detection in its initial stage and reactive detection in the later stage. The proactive detection checks for malicious nodes presence in the initial stage. The reactive detection reduces resource wastage. Secure data Transmission achieved using encryption and shuffling algorithm. Performance of parameters such as Packet Delivery Ratio, End to End Delay, Routing Overhead and Throughput. Compared to DSR ,A2K and ECBDS offers a greater packet delivery ratio, Network Throughput and reduced End to End Delay .In future work, it can be extended for the reducing of Routing Overhead using integrated features of OSPF and RIP protocols.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] A. Po-Chun TSOU,Jian-Ming CHANG, Yi-Hsuan “Developing a BDSR Scheme to Avoid Black Hole

Attack Based on Proactive and Reactive Architecture in MANETs “ICACT2011.

[6] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria,” Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol,” Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145,

[7] Irshad Ullah and Shoaib Ur Rehman,” Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols,” 2010

[8] Akanksha Saini, Harish Kumar, “Effect of Black Hole Attack on AODV Routing Protocol in MANET,”International Journal of Computer Science and Technology

[9] W.Kozma, and L.Lazos,“REAct: resourceefficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103- 110, 2009

[10] W.Wang, B.Bhargava, and M. Linderman, “Defending against Collaborative Packet Drop Attacks on MANETs,” 28th International Symposium on Reliable Distributed Systems September 2009.

[11] Latha Tamilselvan and Dr. V Sankaranarayanan,” Prevention of Co-operative Black Hole Attack in MANET,” Journal of Networks, VOL. 3, NO. 5, MAY 2008.

[12] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala,” A Review of Current Routing Attacks in Mobile Ad Hoc Networks,” International Journal of Computer Science and Security, volume (2) issue (3).

Author Profile

Abdul Jawad PP received the B.Tech degree in Computer Science and Engineering from MG University in 2010 and currently pursuing final year M. Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor under MG University. Research Interest includes Network Security, Cyber Security Education Management and Cyber Forensics.

Bismin Chacko received the B Tech and M Tech degrees in Computer Science and Engineering from MG University, kottayam in 2011 and 2013 respectively. Currently working as Assistant Professor in Computer Science and Engineering Department, KMP College of Engineering, Perumbavoor. Research Interest includes MANETs Security, Information Security and Image Processing.