An Effectual CBHDAP Protocol For Gray Hole And Black Hole Attack Detection Along With A Queuing Technique CBCRTQ For Traffic Management In MANET

Ms. Rashmi T. Ghate[1], Dr. S. V. Sonekar[2]
[1]Assistant Professor, Dept of MMS
[2]HOD, Dept of CSE / IT
[1]RMCET, Ambav (Devrukh)
[2]JDCOEM, Nagpur

Abstract- *Open medium, absence of centralized monitoring point and dynamic topology are various features of MANET. Beside all this, gray hole and black hole are few security attacks in MANET. Here we are going to describe an efficient Crypto-key based Black Hole Detection and Avoidance Protocol (CBHDAP). It generates a group key using Diffie-Hellman key generation algorithm. Then, the generated key is forwarded to the authenticated group members. Before initiating the actual transmission, validation of nodes in the route is done with this key. Various parameters considered in this protocol are Route Reply (RREP), Packet Delivery Ration (PDR) and hop count. To validate the efficiency of this protocol, it is compared with existing protocols.*

In Ad hoc network, nodes travel liberally and separately to be in touch with others from side to side wireless relations, which is represented as bunch of clusters by combining nodes in near proximity with one another. This free movement increases the traffic overhead, so Queuing is one of the important mechanisms in traffic organization. Class Based Cluster Round Trip Queue (CBCRTQ) is an algorithm used for selection of cluster head, which might be used to direct packets in the cluster. Load balancing is done with this technique to manage traffic.

Keywords- CBHDAP; CBCRTQ; Gray hole and Black hole attack; Key exchange; MANET; Traffic management;

I. INTRODUCTION

By the improvement in wireless technologies at a quick pace, there is an importance of keeping the communication protocols unfailing. MANET (Mobile Ad hoc Network) is a wireless network without any infrastructure in which each of the node or the user of node has ability to search the best route. Routing Protocols greatly affect system routine, so the consistency of the protocol in deriving a route is very significant on the resulting QoS (Quality of Services). Multi-hop nature of MANET introduces various attacks leading to failure of security like black hole attack, wormhole attack, sink hole attack, and gray hole attack. Among these different security challenges, black hole attack is a legitimate risk. It is a kind of active attack in which hateful node forwards a fake Route Reply (RREP) packet to the starting node which initiates route detection in order to imagine being a destination node. This attack is launched by malicious node by promoting fresh route with least hop count and peak destination sequence number to the node which initiates route invention.

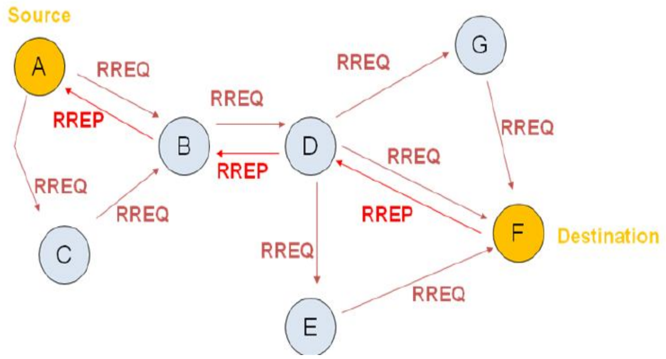

Fig 1 : Route Discovery Process (Ref: www.researchgate.net)

Gray hole attack is somewhat deviation of black hole attack in which hateful node may behave as an sincere node during route invention process and then may change its state to hateful and vice versa. Effective CBHDAP protocol will avoid both these attacks in routing.

CBCRTQ is one of the traffic management algorithm in which messages will be well organized in cluster by selecting cluster head and following the instructions of it.

II. THEORY

A. Mobile Adhoc Network (MANET)

Mobile Ad hoc Network (MANET), is a collection of self-governing mobile nodes that can communicate to each other via radio waves. Movable nodes that are in near proximity of one another can directly communicate, whereas others need the help of midway nodes to route their packets. These networks are entirely dispersed, and can work at any position without the assistance of any infrastructure. Due to this feature these networks highly elastic and strong. Routing will be a challenging task due to random change in MANET. The presented path is rendered incompetent and infeasible. The most important issues for mobile ad hoc networks are routing, medium access control (MAC), and providing quality of service and security. This article addresses the routing problem in a mobile ad hoc network (MANET) without considering the other issues like security and medium access control. Routing in MANET means the designed flow of data from source to destination with utmost network performance.

The characteristics of these networks are summarized as follows:

- Communication via wireless Network.
- Absence of centralized director and infrastructure.
- Active network topology.
- Regular routing updates.
- Nodes can work both as hosts as well as routers.
- Built-in mutual trust.

Few applications of MANETs are

- Tragedy relief operations.
- Defense Development.
- Insistent Business meetings.
- Mine place operations.

B. Black hole Assault

Black hole assault is a very serious problem in MANET, because it affects security. During the route discovery process, malicious node shows highest destination sequence number and shortest path towards the destination. Source node will select it as an intermediate node to forward packets to destination. It will drop or consume that packet and do not allow forwarding it to the next node. It may affect uninterrupted delivery ratio, packet release ratio and throughput.

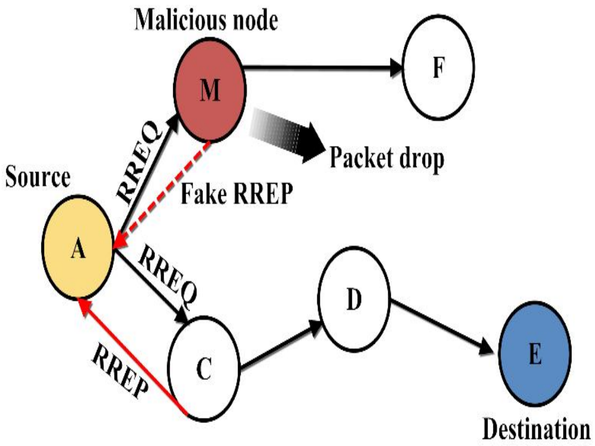

Fig 2: Black Hole Attack (Ref: www.slideplayer.com)

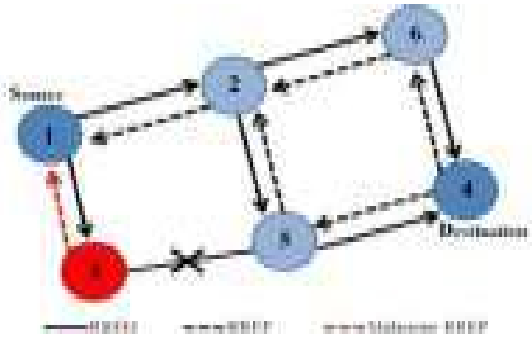

Fig 3: Single Black Hole Attack (Ref: hcis-journal.springeropen.com)

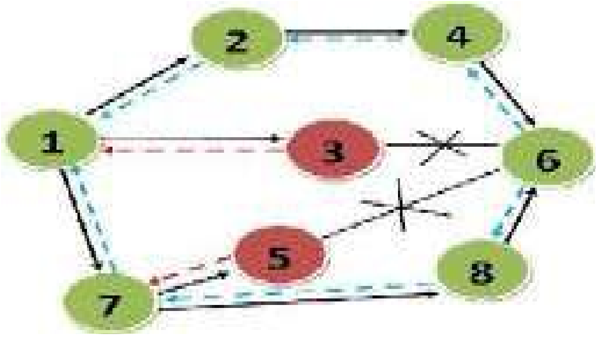

Fig 4: Collaborative Black Hole Attack (Ref: www.ijser.org)

Multiple techniques like MEAODV, Modified Enhanced Ad hoc On-demand Distance Vector, GBHASM, Grouped Black Hole Attack Security Model, MDSR, Modified Dynamic Source Routing, etc. are available for black hole attacks detection. These techniques detect only collaborative black hole assault, whereas CBHDAP protocol will detect single black hole assault as well.

C. Gray hole Assault

A variation of black hole assault in which hateful node behaves as a truthful node during route invention and then may change its state to hateful and vice versa is said to be an gray hole attack. That hateful node might drop some or all of the data packets. Due to congestion overload and capability of changing states, it is difficult to detect gray hole attacks. CBHDAP protocol will help to detect the current state of node i.e. whether it is malicious or honest.

D. Traffic Management

As nodes moves freely and independently in wireless network, it increases the traffic overhead. In such a heavy traffic, there are lot many chances of collision and loss of packets. To avoid this one must manage the traffic efficiently by using a queuing technique, because all the packets are of same capability. For successful delivery of packets to the destination, a queuing technique must be used in a cluster. CBCRTQ is one of the best options of queuing technique. Due to same capability, convinced nodes are chosen to form the cluster heads.

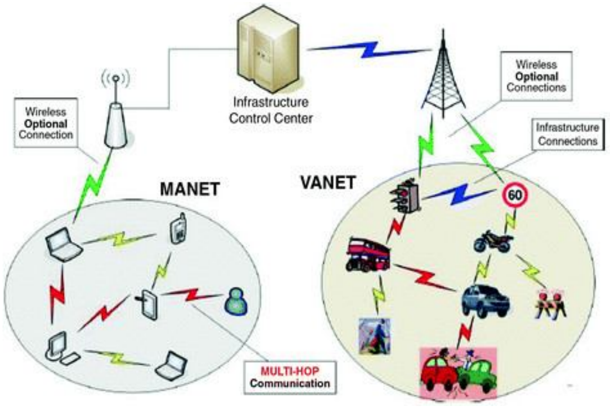
Wireless Optional Connection
Infrastructure Control Center
Wireless Optional Connections
Infrastructure Connections
MANET
VANET
60
MULTI-HOP Communication

Fig 5: Traffic Management (Ref: www.researchgate.net)

E.CBHDAP Protocol

CBHDAP i.e. Crypto-key based black hole detection and avoidance protocol is used for detection and avoidance of single plus collaborative black hole and gray hole assault. The fundamental goals of it are:

- To execute key agreement detection algorithm for finding nearness black hole assault and gray hole assault in MANET.
- To avoid black hole assault and gray hole assault by accepting the parameters like hop count, packet delivery and time.

A general stream of CBHDAP protocol is shown below which includes following steps:

- Network formation
- Group key sharing
- Route discovery
- Packet transmission

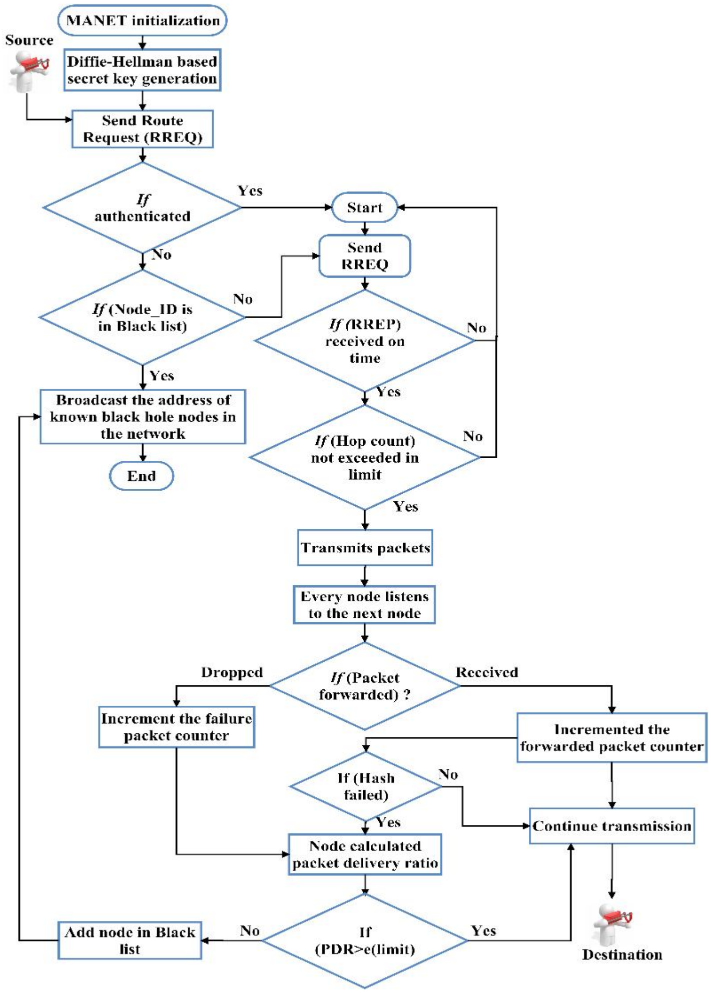
MANET initialization
Source
Diffie-Hellman based secret key generation
Send Route Request (RREQ)
If authenticated
Yes
No
Start
Send RREQ
If (Node_ID is in Black list)
No
Yes
If (RREP) received on time
No
Yes
Broadcast the address of known black hole nodes in the network
End
If (Hop count) not exceeded in limit
No
Yes
Transmits packets
Every node listens to the next node
Dropped
If (Packet forwarded) ?
Received
Increment the failure packet counter
Incremented the forwarded packet counter
If (Hash failed)
No
Yes
Continue transmission
Node calculated packet delivery ratio
Add node in Black list
No
If (PDR>e(limit)
Yes
Destination

Fig 6: Overflow of CBHDAP Protocol

1) The 1st step of CBHDAP protocol is network formation with 100 no of nodes by using NS2 tool.
2) The 2nd step is to generate group key by using Diffie-Hellman algorithm. This key is shared by nodes in the network that enables communication between group members.
3) The 3rd step is route discovery in which estimation of optimal route between sender and receiver is done. This estimation is based on 2 steps such as:

3.1) Node Authentication:

Authenticity is based on 2 metrics such as time and hop count. First we have to decide conceivable path to the destination, then source node broadcasts RREQ message, then neighboring nodes evaluate the count of hops required to arrive at destination and sends RREP message. If time interval between RREQ and RREP message satisfy the Time to Live (TTL), then the corresponding neighboring node is considered as authentic else it is considered as unauthentic and added to black list. Another metric to check authenticity is hop count. In the RREP message, every neighboring node sends the count of number of nodes required for transmitting data from source to destination in the form of hop count. If hop count exceeds the hop limit, then corresponding node is considered as unauthentic and added to black list.

3.2) Black list verification:

Black list is a list which contains ID of malicious nodes obtained from the history of previous attacks. Every node in the network maintains this list. Before forwarding RREQ message by the source node, it first verifies its black list and then sends message to the nodes that are not in black list.

4] In 4th step the actual packet transmission is initiated. During this transmission every node listens to the next node. Successful transmission of packet increments the forwarded packets counter whereas unsuccessful transmission increments the failure packets counter. To avoid black hole attack, hash value of the packet is validated. If hash value fails, then it indicates non appearance of black hole attack and hence transmission is continued, or else PDR is calculated. If PDR is greater than the limit, then it indicates that there is no packet drop hence transmission is continued else this node is added to the black list

F.CBCRTQ Protocol

Group of nodes in the close proximity of one another is termed as cluster, whereas the process of forming clusters is termed as clustering. Cluster Head (CH) is selected from every cluster based on their priority and capability. Each CH acts as a manager within its zone. Each router in the network must implements some queuing discipline which governs how packets are buffered for communication. Therefore queuing is one of the significant mechanisms in traffic management.

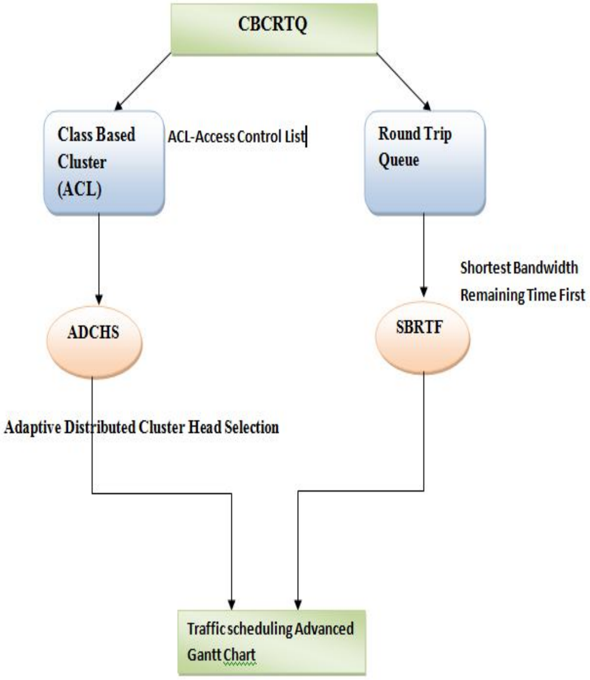
CBCRTQ
Class Based Cluster (ACL)
ACL-Access Control List
Round Trip Queue
Shortest Bandwidth Remaining Time First
ADCHS
SBRTF
Adaptive Distributed Cluster Head Selection
Traffic scheduling Advanced Gantt Chart

Fig 7: Classification Diagram of CBCRTQ

III. RESULT AND ANALYSIS

This section indicates the behavior and result of CBHDAP protocol for detection and avoidance of black and gray hole assault. Performance of Adhoc On demand Distance Vector (AODV), Modified Reverse AODV (MRAODV) and Dynamic Source Routing (DSR) are compared based on several parameters like Packet Delivery Ratio (PDR), Throughput, Routing Overhead, E2E Delay, Node Outage Count, Detection of attacks, Energy consumption and Packet Transfer Rate.

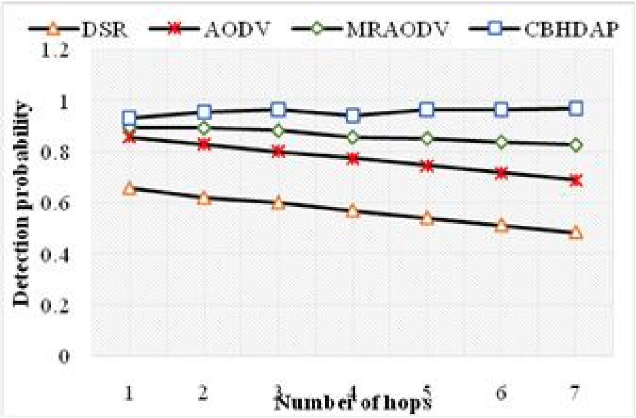

Fig 8: Comparison of detection of black hole nodes for the existing and proposed protocols

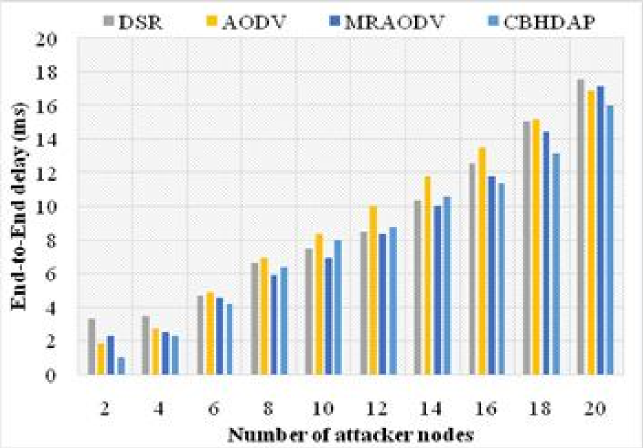

Fig 9: Comparison of End-to-End delay for the existing and the proposed protocols

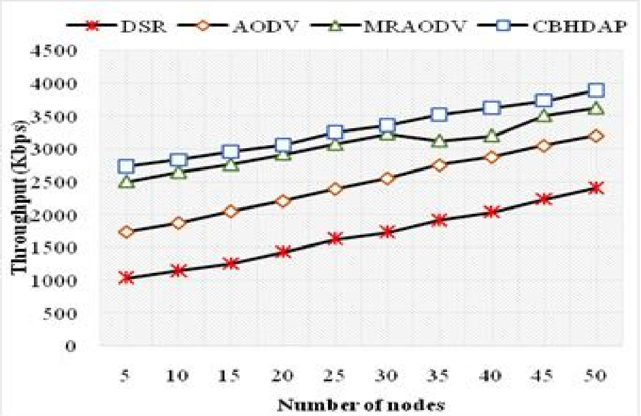

Fig 10: Comparison of throughput for the existing and the proposed protocols

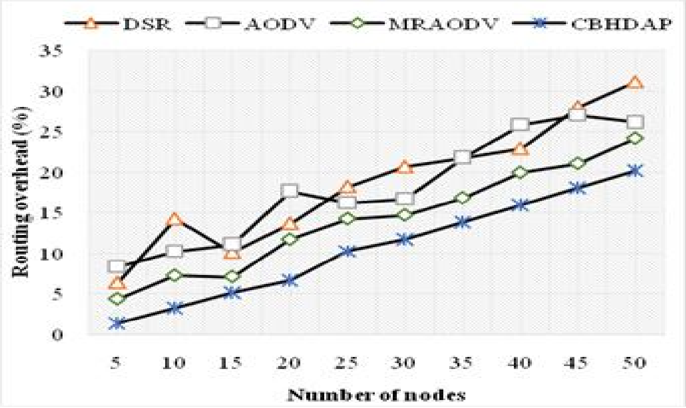

Fig 11: Comparison of routing overhead for the existing and proposed protocols

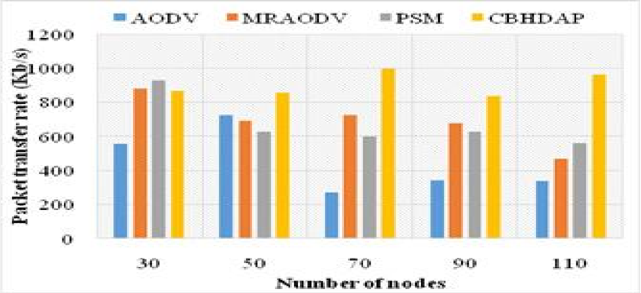

Fig 12: Comparison of packet transfer rate for the existing and the proposed methods.

IV. CONCLUSION AND FUTURE WORK

From the above compared outcome we can clearly conclude that CBHDAP is an effectual algorithm for detecting and avoiding attacks like black hole and gray hole. Initially sender uses Diffie-Hellman algorithm for generation of group key, which is shared between group members. The actual transmission is initiated by broadcasting RREQ message. After receiving RREQ message, every neighboring node sends RREP message. If RREP is found unauthentic, the corresponding node ID is added to the black list and address of it is broadcasted to remaining group members. On the other hand, if RREP is authentic, the time gap in between RREQ and RREP is checked. If it exceeds TTL then node is added to black list, else it checks hop count of all neighboring nodes. If hop count is satisfactory, the transmission is initiated.

The Reduced traffic in VoIP and time consumption of wireless sensor node increases the network life time because traffic has not been used for whole time instead it is used for particular time in CBCRTQ protocol. Hence, we can clearly conclude that CBCRTQ is an efficient queuing technique used for traffic management in MANET.

V. ACKNOWLEDGEMENT

Abbreviation	Full Form
MANET	Mobile Ad-hoc Network
MAC	Medium Access Control
QoS	Quality of Service
RREP	Route Reply
RREQ	Route Request
CBHDAP	Crypto-key based Black Hole Detection & Avoidance Protocol
CBCRTQ	Class Based Cluster Round Trip Queue

AODV	Ad-hoc On-demand Distance Vector
SAODV	Secure Ad-hoc On-demand Distance Vector
DPRAODV	Detection, Prevention & Reactive AODV
REAct	Resource Efficient Accountability
DSR	Dynamic Source Routing
PDR	Packet Delivery Ratio
DRI	Data Routing Information
DCM	Distributed Cooperative Mechanism
SN	Source Node
IN	Intermediate Node
NHN	Next Hope Node
PRF	Pseudo Random Function
MAC	Message Authentication Code
PKI	Public Key Infrastructure
BBN	Backbone Nodes
RIP	Restricted IP
BDSR	Bait DSR
VoIP	Voice over Internet Protocol
CH	Cluster Head
ADCHS	Adaptive Distributed Cluster Head Selection
SBRTF	Shortest Bandwidth Remaining Time First
UDP	User Datagram Protocol
VGA	Video Graphics Array
NAM	Network AniMator
NS2	Network Simulator (Version 2)
OTcl	Object-oriented Tool Command Language
Tcl	Tool Command Language
TclCL	Tool Command Language with classes

REFERENCES

[1] Somasundaram K , Vijaya Kumar K. Study of reliable and secure routing protocols in MANET. Indian Journal of Science and Technology. 2016; 9(14):1–10.

[2] Usha G , Babu RM. A Novel Honey pot Based Detection and Isolation Approach (NHBADI) for Black Hole Attacks in MANET. Wireless Personal Communications. 2016; 1–15.

[3] Dorri A. An EDRI-based approach for eliminating and detecting cooperative black hole nodes in MANET. Wireless Networks. 2016; 11(1):1–12.

[4] Somasundaram K , Vijaya Kumar K. Detection of black hole assaults in MANET by using proximity set method. International Journal of Information Security and Computer Science. 2016; 14(3):136–45.

[5] Arora SK, Vijan S, Gaba GS. Detection and analysis of black hole assault using IDS. Indian Journal of Technology and Science. 2016; 9(20):1–5.

[6] Ghazvini M, Shahabi S, Bakhtiarian M. A modified algorithm to improve performance and security of AODV protocol against black hole attack. Wireless Networks. 2015; 22(5):1–7.

[7] Thangadurai K , Anchugam CV. Detection of Black Hole Attack in MANET using Ant Colony Optimization – simulation Analysis. Indian Journal of Technology and Science. 2015; 8(13):1–10.

[8] Singh U, Arya N, Singh S. Detecting and avoiding of wormhole attack and collaborative black hole attack in MANET using trusted AODV routing algorithm. International Conference on Computer, Communication and Control (IC4), India. 2015. p. 1–5.

[9] Kumar R, Kumar V. An Adaptive Approach for Detection of Black hole Attack in Mobile Ad hoc Network. Procedia Computer Science. 2015; 48:472–79.

[10] Priyan MK, Balan EV, Gokulnath C, Devi GU. Fuzzy Based Intrusion Detection Systems in MANET. Procedia Computer Science. 2015; 50:109–14.

[11] Kancherla S , Vijaya Kumar K. An empirical model of malicious node detection and prevention with data rating. International Journal of Engineering Trends and Technology. 2014; 2(17):56–9.

[12] Krishnamurthi I , Mohanapriya M. Modified DSR protocol for removal and detection of selective black hole

attack in MANET. Computers and Electrical Engineering. 2014; 40(2):530–8.

[13] Olmos MDS, Hernandez-Orallo, Cano J-C, Manzoni P , Calafate CT. A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. Wireless Personal Communications. 2014; 74:1099–116.

[14] Nag T, Biswas S, Neogy S. Trust based energy efficient de-tection and avoidance of black hole attack to ensure secure routing in MANET. Innovations and Applications in Mobile Computing (AIMoC), Kolkata, India. 2014; 157–64.

[15] Kanthe AM, Wahane G, Simunic D. Detection of cooperative black hole attack using crosschecking with true link in MANET. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Zagreb. 2014. p. 1–6.

[16] M. Vijayakumar and V. Karthikeyani, "Intelligent adaptive energy efficient & effective signal buffer management algorithm for VoIP (QOS) over MANET", International journal of future generation communication and networking, vol.9, no. 1, **(2016)**, pp. 47-60.

[17] Jagdish J. Rathod , Amit Lathigara," Novel Approach of Preventing and Detecting Gray Hole Attack on AODV based MANET", Volume 3, Issue 1, January 2015.

[18] Sandeep Kumar, Mrs. Sangeeta Pramod Kumar Soni," A Review on Gray Hole Assault in MANETs", Volume 4, Issue 9, September 2014.

[19] Vinod kumar and Pooja. ," A Review on Detection of Black hole Attack Techniques in MANET' 'International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 4, pp.364-368, 2014.

[20] Neeraj saini , lalit Garg ," Enhanced AODV Routing Protocol against Black hole Assault'',International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 6, pp.847-850, June 2014.