www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7106-7111

Analysis of Reactive Attacks on Mobile Communication Protocol Network

Praveen Kumar Maurya[1], Akhilesh Panday[2]
[1]**Master of Technology (Scholar), Suresh GyanVihar University, India, praveen.kumar.maurya16@gmail.com**
[2]**Assistant Professor, Suresh GyanVihar University, India, akhileshmtech10@gmail.com**

ABSTRACT

Abstract -A MANETs (Mobile Ad-Hoc N/W) are De-Centralized wireless linkages networks through the Self-configuring mobile ad hoc nodes. These networks are vulnerable to protection threats, caused by the nonattendance of trusted central authority or directness of network topology. Black hole attack is among the path interruption attacks that origin a better harm to the network. A hateful node disprove that it is having shortest pathway and traps packets in that way demeaning network performance in this attack. MANETs create a better confront for routing protocols. Mainly of the routing protocols for MANETs are therefore susceptible to a variety of categories of the attacks. Ad hoc on-demand space (distance) vector routing is extremely accepted routing algorithm. Nevertheless, it is exposed to the renowned black hole attack, where a hateful node mistakenly advertises fine paths to an objective node throughout the route detection procedure .This attack takes a form of extra ruthless when a group of hateful nodes collaborate every one other. It is a proficient routing protocol however it require with protection issues in this paper that's why AODV (Ad hoc On Demand Distance Vector Routing) protocol is utilized for route founding. A protection method is obtainable in opposition to a harmonized attack by numerous black hole nodes in a MANET. The simulation performed on the projected scheme has formed outcomes that express the efficiency of the method in discovery of the attack whereas maintaining a rational level of through position in the network.

Key words:Black Hole,AODV, E-mail, Network, OPNET 4.5, Performance Parameters, Security etc.

1. INTRODUCTION

A network is an interconnection of computers and devices for the purpose of communication and sharing of resources between users. It can be a wired network or a wireless one. With advancement in communication technology and changing lifestyles, there has been increased demand for wireless medium of networking. These wireless networks are infrastructure based but in situation where connectivity is needed and there is no base station, an ad hoc network is used. An ad hoc network is a network characterized by the absence of a fixed infrastructure. Ad hoc network is used in situation where cabling cost is to be eliminated and stations exchange information independently of the environment or situation like disaster operations etc. Nodes in ad hoc network should have the additional feature of routing packets, security, Quality of Services over and above the normal function of receiving and transmitting data.

1.1MOBILE AD HOC NETWORK

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links [19]. There is independent movement of devices. Due to mobility of devices, link breakage is frequent and so topology changes rapidly and unpredictably with time.

Mobile devices forward messages between devices as such acts as router and carry out their own processing of data like a normal host. They may operate in a standalone
Fashion, or may be connected to a larger network [4]. In MANET, the address is tied to the devices, not the topological location, as it is infrastructure less. Routing node carries with it an address or an address prefix. So when node moves, it moves its actual address also. The change in topology demands for recalculation of routing.

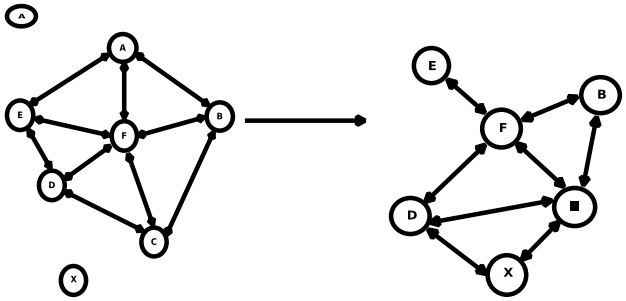


Figure 1.1: MANET - Dynamic Topology

1.2 MANET ROUTING

Every node in the network maintains a node through which it can reach a destination in an optimal way. A data packet contains final destination in its header. Every time it pass through intermediate node in the network between source and sink, current node checks for the final destination in the header and relay it to the preferred neighbor for the destination. This forwarding continues till it reaches the final destination. Mechanism for construction, maintaining and updating of routing tables differs from one routing method to another but

with the sole purpose of finding an optimal path to reach the destination. Next hop routing method can be classified into

1. Link State
2. Distance Vector

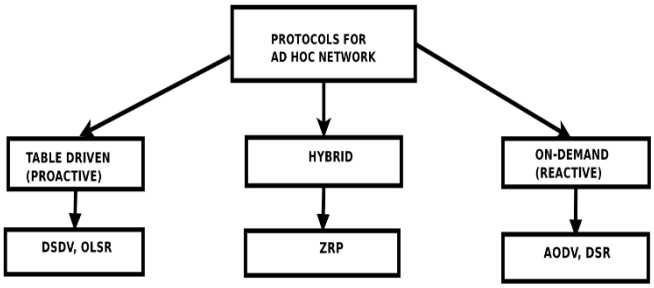
- **Link State:** Every node maintains a view about the path reachable by all other nodes in the network. Maintenance of this view is achieved by periodically broadcasting the link cost of its outgoing links to all other node in the network. Flooding protocol is used for the broadcast of outgoing link cost. When other node receives this information, it updates its view and applies shortest path algorithm to choose its next hop neighbor with itself as the root.
- **Distance Vector:** Each node maintains for every destination a set of distances. Next hop neighbor is chosen on the basis of the minimum hop count to reach a particular destination through a node. Node monitors cost of its outgoing links and periodically broadcast to each one of its neighbor, its current estimate of the shortest distance to every other node in the network. In this manner distance information is kept up-to-date.

A. *1.2.1*Routing Protocol

An ad hoc mobile network is a collection of mobile nodes those are dynamically and arbitrarily located and interconnections between these mobile nodes changes with time. The question arises how do these nodes communicate with each other? How is the routing decision taken? The answer to this is routing protocol. They are a set of rules which specifies how routers communicate with each other, disseminate information which enables them to select routes between any two nodes in the network. The choice of route selection is done by routing algorithms.

Routing protocol is used to discover routes between nodes and facilitate communication between nodes in the network. The primary goal of routing protocol is to obtain correct and efficient route establishment between a pair of source and destination nodes for timely delivery of messages. It also defines the set-up, indicating, enactment and broadcast of information in excess of a communication medium. Each node has prior information about networks attached to it directly. This information is first shared among immediate neighbors and is then propagated throughout the network with time. In this way information about the network is gained. Routing protocol employs different algorithm accordingly. The general performance measures are delay and throughput of information [20]. Construction of routes is constrained by limited bandwidth and should be done with minimum bandwidth and overhead. Path reliability is also used as a performance metric to distinguish ad hoc network based on the distribution of nodes

Routing protocol can be broadly classified as proactive, reactive and hybrid as shown in Figure 1.2. Proactive predetermines the routes and reactive determines routes only when needed while hybrid provides the combine feature of both proactive and reactive.



- **Proactive (Table-Driven)**: Proactive protocols maintain routing information from the start. They refresh the entry after every specified time intervals. It provides fast response to topology changes in the network as it maintains routing information for all other network destinations and react to changes in the network. It incurs the overhead of signaling information as it also maintains routing information of some destination which is of no interest. Some Proactive protocols are Destination Sequence Distance Vector (DSDV), Optimized Link State Routing (OLSR) etc.
- **Reactive (On-Demand)**: Reactive protocol provides information on need basis and signaling overhead incurred in the case of proactive routing protocols is reduced. But it takes more time for route establishments as compared to proactive ones. Reactive protocols are Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) etc.

Hybrid: Hybrid protocols combines table-driven with on-demand routing protocol [12]. It uses proactive routing when it want to reduce the delay in small networks and uses reactive in larger network in order to reduce the overhead of maintaining the table data. Organizing the network according to network parameter is the complexity of hybrid protocol. Zone Routing Protocol (ZRP) is hybrid routing protocol. Each node keeps a record of routing information for its own zone.

2. BACKGROUND

MANET is an extremely vibrant network, there is a vast range of MANET applications which make it perfect to utilize. It is extremely effortless to arrange negligible deal of MANET in emergencies similar to natural calamity region makes it extra appropriate.

A huge study work has been finished on the presentation assessment of mobile ad-hoc network routing protocols utilizing NS-2.Some different methods and simulator provides numerous different outcome for routing protocols performance. We require to a stare in an immense outlook for the contact of routing protocols which are not reflected in a fastidious atmosphere. The thought of this project is to ponder on the performance of AODV, OLSR and TORA MANET protocols on OPNET Modeler 14.5. For all these study we will utilize HTTP, FTP, E-MAIL and Voice traffic to display the analysis and attacks in to the wireless network as well as for the contact of ad hoc network routing protocols for recreation.

3. REALTED WORK

MANET is very abundant prevalent in line for to the circumstance that these systems are self-motivated, infrastructure a smaller amount and scalable. Regardless of the statistic of acceptance of MANET, these networks are precise much unprotected to attacks. Wireless relations also makes the MANET extra vulnerable to attacks which create it stress-free for the attacker to go confidential the network and become right of entry to the constant communication. Dissimilar types of attacks have been examined in MANET and their conclusion on the network. Violence such as gray hole, where the attacker node conduct yourself maliciously intended for the time while waiting for the packets are released and at that time change to their usual performance. MANETs routing protocols are similarly being broken by the attackers in the procedure of flooding attack, which is completed by the attacker one or the other by means of RREQ or data flooding.

In any linkage, the despatcher needs its documents to be conducted as soon as imaginable in a protected and fast route, several attackers announce themselves to have the direct and in height bandwidth accessible for the broadcast such as in wormhole attack, and the invader becomes themselves in solid planned position in the network. They create the procedure of

their position i.e. they have direct track among the nodes. One of the greatest ascending matters in MANET is the partial battery, attackers receipts an benefit of this fault and attempts to hang onto the nodes awake while waiting for all its energy is misplaced and the node go into stable sleep. Several other attacks MANET such as jellyfish attack, adjustment attack, misrouting attack and Routing Table Excess have been deliberate and unprotected.

In to the black hole attack, a malicious node usages its routing protocol in command to promote itself for consuming the direct track to the last stop node or to the packet it requirements to intercept.

This aggressive node promotes its accessibility of renewed routes regardless of examination its routing table. In this approach attacker node will permanently have the accessibility in responding to the path demand and thus interrupt the data packet and recollect it. This thesis emphases on the study the impression of Black Hole attack in MANET by means of both Reactive and Proactive procedures and to associate the liability of both these protocols in contradiction of the attack.

4. SIMILATION TOOLS

The tool utilized for the simulation lessons is OPNET 14.5 modeler. OPNET is a network and application based software utilized for network management and breakdown [24]. OPNET models communication devices, a variety of protocols, construction of unlike networks and technologies and offer simulation of their performances in implicit surroundings. OPNET supplies a variety of explore and growth explanation which helps in study of breakdown and upgrading of wireless technologies similar to WIMAX, Wi Fi, UMTS, breakdown and scheming of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks.

In our casing we utilized OPNET for modeling of network nodes, selecting its figures and after that running its simulation to dig up the outcome for breakdown.

5. PERFORMANCE METRICS

OPNET is not the same limitations for performance assessment of the MANET network arrangements further down dissimilar transmitting protocols. To do again the black hole occurrence, we bring into being with the general idea of presentation metrics selected for the assessment that take in End point delay, Throughput and Linkage load. In addition, putting into practice of the reproduction arrangement and its project are illuminated.

1. Throughput

Output characterizes the entire traffic flow fruitfully established and accelerated to the innovative coat by means of the WLAN MAC. The situation is the percentage of entire quantity of documents which influences the mouthpiece on or after the despatcher to the period it receipts in place of the receiver to take delivery of the last packet data. It is characterized in moments per second or data packets/sec. In to the MANETs traffic output is affected by way of a number of variations in topology, some degree of bandwidth and some degree of power. Unpredictable communication is similarly one of the influences which unpleasantly have emotional impact the throughput limitation.

2. End-to-End delay

The data packet end point delay is the normal time in instruction to negotiate the data packet privileged the system network. This take account of the time period from producing the data packet as of despatcher up till the response of the data packet by end point receiver or last stop and communicated in last seconds. This take account of the overall delay of traffic networks as well as buffer queues, broadcast interval and talk into delay in line for to routing happenings. Not the same application requirements dissimilar data packet interruption level. Vocal sound and video broadcast have need of less significant delay and illustration minimum tolerance to the interruption level.

3. Load

The network load, the situation is the over-all traffic acknowledged by the complete network as of upper level of MAC which is recognized and get in line for broadcast. It point out the measure of traffic flow in whole network. It characterizes the entire documents traffic in moments per seconds established by the complete network as of upper layer recognized and form a queue for broadcast. It make sure of not consist of any sophisticated layer documents traffic forbidden without queue up in line for to outsized data package proportions.

6. SIMULATION SETUP

Figure works the simulation setup of a first scenario comprising of 50 mobile nodes moving at a continuous speed of 10 meter/seconds. All scenarios have been established, all of them with mobility of 10 meter per seconds. Numbers of mobile nodes were varied and simulation period was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is in use exponential (1) and its packet size (bits) is exponential (1024). The data rates of wireless mobile nodes are 11 Mbps with the default transferring power of 0.005 watts. Random way point mobility is selected with continuous speed of 10 meter/seconds and with pause time of content 100 seconds. This pause time is occupied after documents reaches the end point only. Our aim was to conclude the protocol which displays less vulnerability in circumstance of black hole attack. We pick out AODV and OLSR routing protocol which are reactive and proactive protocols correspondingly. In both case AODV and OLSR, malevolent node buffer size is let down to a level which rise packet deW drop. Furthermore the simulation limitations are specified in Tables

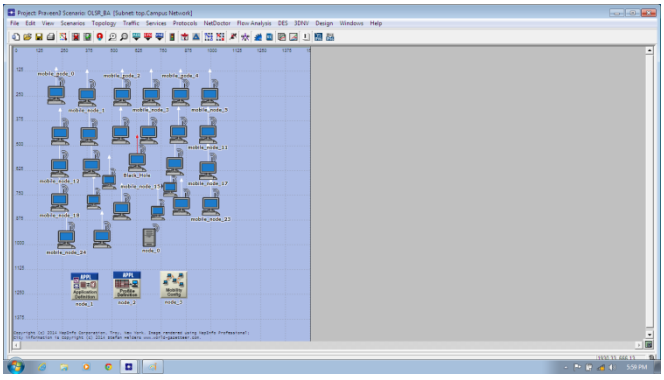


Fig. nods setup with black hole node

7. ANALYSIS AND RESULTS

A wireless network are of 30 nodes and the file size of 20000 bytes (for E-MAIL),happening to a (2000×2000) squaremeter area.This paper represent the scenarios of 30 nodes which are simulated by taking Reactive routing protocols and showing attacks and their delay, network load and throughput etc. The reproduction time is 360sec for all circumstances.

4.6 RESULTS

In this chapter attentions on outcome and its investigation based on the simulation accomplished in OPNET modeler 14.5. Our simulated results are provided in Figures gives the dissimilarity in network nodes although under Black Hole attack.

4.1 Packet End-to-End Delay

Packet end-to-end delay in circumstance of Black Hole attack and without attack be determined by on the protocol routing technique and number of nodes elaborate.
In case of 30 nodes the delay is 5 percent further as associated to the event of 26 nodes..

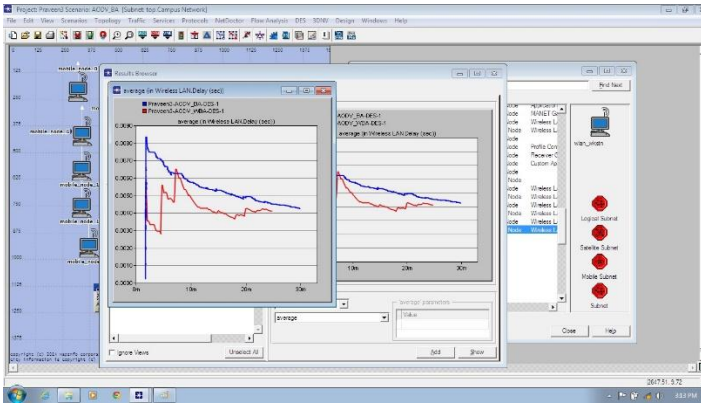


Fig.4.2 End-to-end delay of 26 nodes AODV with vs. without attack

Throughput

The equivalent is observed in the situation with AODV, without attack, this one throughput is greater than in the case with further down attack for the reason that of the packets rejected by the malicious node. Correspondingly in Fig. for 30 nodes, the throughput is higherfor the reason that of the greater number of nodes but the tendency of throughput through attack and without attack remains the equivalent as in 26 numbers of nodes.

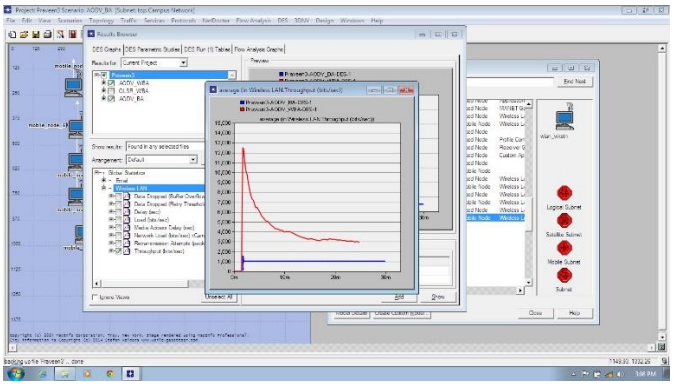


Fig.4.3 Throughput of AODV with vs. without attack for 26 nodes

We have detected that the greater number of sources providesa reduced amount ofdissimilarity in throughput as compare to a smaller amount of number of sources. This is for the reason that the greater the number of sources is the extrajamming there is. As throughput is the percentageof the entire data established from source to the time interval it receipts till the receiver collects the last packet. A lesser delay transforms into greater throughput.

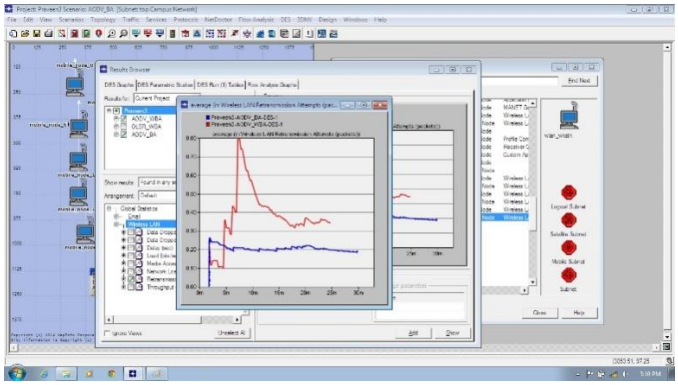


Fig.4.4 Transformation 26 nodes AODV with vs. without attack

7.3 Download response time

In case of 26 nodes the network load of AODV is 30 times greater in case of without attack which indicates that it is essentially routing its packet wholatergetappropriately. But below attack it cannot refer its packet i.e. packet disposal indications to a decrease of network capacity.

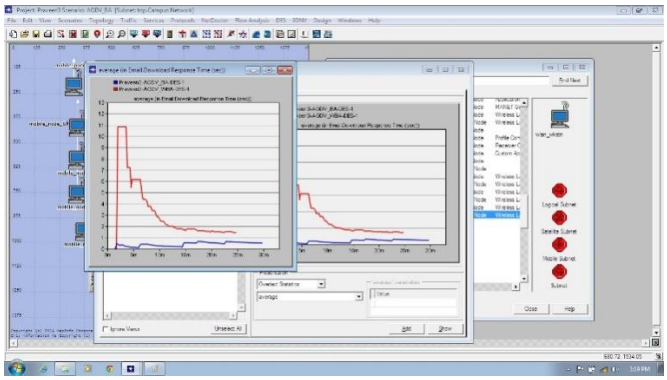


Fig.4.5 Network Capacity of AODV with vs. without attack for 26 nodes

Traffic Received

The network contents diagram of AODV with and without presence of a malicious node has been accessible in the Fig. The network load of OLSR is significantly in height as equivalent to AODV.

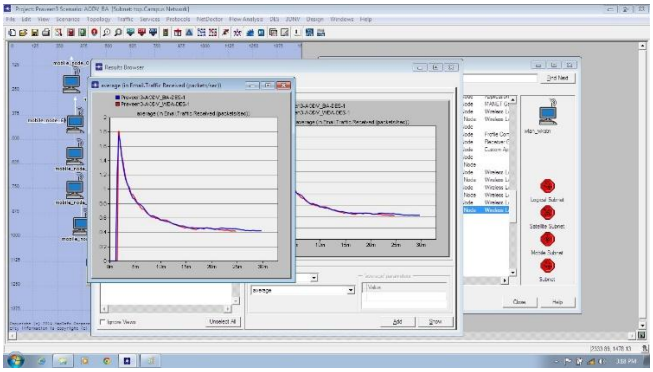


Fig.4.6 Traffic received of AODV with vs. without violence for 30 nodes

Retransmission Attempts

In the analysis of the AODV with and without attack network analysis is show the retransmission
Of the network. We considered the attempt of the network for the analysis of the transmission. In
The mobile ad hoc network is perform the retransmission of the network in AODV protocol.

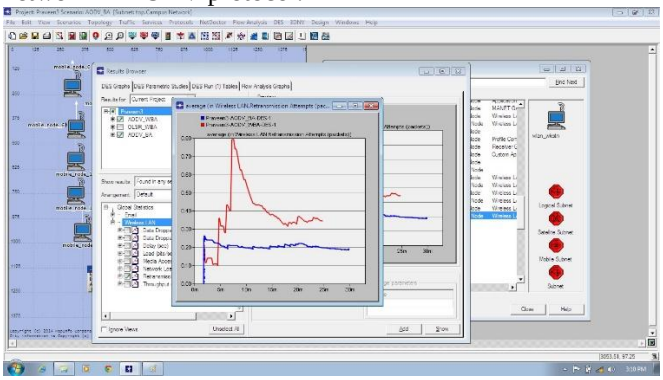


Fig.4.7 Retransmission attempt wireless lan of AODV with and without attack

In circumstance of network contents Fig. and displays that OLSR has a great network capacity in occurrence of a malicious node as associate to that of AODV. Through 26 nodes and 50 nodes OLSR has in altitude network load for the reason that the routing protocols are capable to modify its variations in it throughout node resume and node take a breather. This is dissimilar at changed speeds, at in elevation speeds the routing protocols takingsconsiderableextra time for modifying and subsequently sending of traffic to the new ways. In circumstance of greater number of nodes AODV counter more rapidly as parallel to OLSR which prepared the modification in network load considerably comprehensive. As the node bring into being to pause and resumes and its mobility subsequently the beginning period consuming further stability make network capacity extra noticeable.

8. Conclusions and Future Works

Due to the inherent design drawbacks of routing protocol in MANETs, several researchers have accompanied miscellaneous techniques to recommend different types of prevention mechanisms for black hole problems.
In this paper, we first summary the pros and cons with prevalent routing protocol in wireless mobile ad hoc networks. Then, the state-of the-art routing approaches of current explanations are characterized and deliberated. The suggestions are presented in a sequential order and separated into single black hole and collaborative black hole attack.

According to this work, we notice that both of proactive routing and reactive routing have particular skills. The proactive finding technique has the superior packet sending ratio and precise detection probability, but underwent from the advanced routing overhead due to the from time to time broadcast packets. The reactive recognition method removes the routing overhead problem from the event-driven approach, but suffered from several packet loss in the start of routing process. Therefore, we mention that a hybrid recognition method which collective the advantages of proactive routing with reactive routing is the tendency to upcoming research direction. However, we also determine that the attacker's misconduct action is the main factor. The attackers are able to avoid the detection mechanism, no matter what types of routing recognition used.
Therefore, some key encryption approaches or hash-based methods are broken to resolve this problem. The black hole problems are quiet a dynamic investigation area. This paper will advantage of more investigators to understand the present-day status rapidly. We tried to find out and investigate the property of Black Hole attack in MANETs by means of reactive routing protocol AODV and proactive routing protocol OLSR. A bundle of research effort is still required in this region. There is requiring investigating Black Hole attack in additional MANETs routing protocols such at the same time as DSR, TORA and GRP. Other category of attacks such the same as Wormhole, Jellyfish and Sybil attacks require to exist deliberate in evaluation with Black Hole attack. They can be there sort out on the foundation of how to a large extent they have an effect on the presentation of the arrangement. Black Hole attack can furthermore attack the new way surrounding i.e. as an interruption attack. The impact investigation and recognition of this performance of Black Hole attack as well as investigation of the finest removal move toward for such actions has to be approved away from home for further investigate. Future works furthermore include the request of the show aggression and defense hierarchy line of attack in a variety of dissimilar domain to take in outside safety circumstances and unusual protection attacks on MANET. Upcoming research be supposed to also include automate the procedure of analyzing protection in MANET by means of do violence to and defense trees. Libraries of standard attack and defense would apparently require to be produced to remain the troubles scalable. Technique of maintenance these libraries updated furthermore have need of to be developed.

ACKNOWLEDGEMENT

We would like to thanks all the friends, staff member and our guide of Computer science and Information Technology department of Suresh GyanVihar University for giving us their precious time and facilities which is necessary for this research.

REFERENCES

[1] Burbank JL, Chimento PF, Haberman BK, Kasch WT (2009) Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communication Magazine 44(11):39–45. doi: 10.1109/COM-M.2006.248156

[2] Sarma N, Nandi S (2010) Service differentiation using priority-based MAC protocol in MANETs. International Journal of Internet Protocol Technology 5(3):115–131. doi: 10.1504/IJIPT.2010.035383

[3] Ting H-C, Chang R-S (2003) Improving the Performance of Broadcasting in Ad Hoc Wireless Networks. Journal of Internet Technology 4(4):209–216

[4] Liao W-H, Tseng Y-C, Lo K-L, Sheu J-P (2000) GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID. Journal of Internet Technology 1(2):22–32

[5] Yang S-J, Lin Y-C (2009) Static and Dynamic RED Tuning for TCP Performance on the Mobile Ad Hoc Networks. Journal of Internet Technology 10(1):13–21

[6] E.Perkins, E. M. Royer, S. R. Das, and M. K. Marina,"Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," IEEE Personal Communications, February 2001,pp. 16-28.

[7] HumairaEhsan and Zartash Afzal Uzmi, "Performance Comparison of Ad-hoc Wireless Network Routing Protocols", IEEE Transactions, 2004.

[8] Y.-C. Hu, D. B. Johnson, A. Perrig, ―SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks,‖ Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, Jun. 2002, pp. 3-13.

[9] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[10] Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004