Performance Analysis of Black Hole and Worm Hole Attacks in MANETs

Mazoon Hashil Al Rubaiei[1], Hothefa Shaker Jassim[1] and Baraa T. Sharef[2]

[1]Modern College of Business and Science, Al-Khuwair, Muscat, Oman
[2] Information Technology Department College of Information Technology, Manama, Bahrain.

***Abstract*:** A Mobile Ad Hoc Network MANET is compost of freely and mobility set of mobile nodes. They form a temporary dynamic wireless network without any infrastructure. Since the nodes act as both host and router in their communication, they act as a router provide connectivity by forwarding data packets among intermediate node to the destination. Routing protocol is used to grove their communication and connectivity as an example, Ad On-demand distance vector (AODV) routing protocol. However, due to the lack of security vulnerabilities of routing protocols and the absence of infrastructure, MANET is vulnerable to various security threats and attacks. This paper examines the impact of two types of attacks on AODV routing protocol using Network Simulator version 2 (NS2) environment. These attacks are Blackhole and Wormhole Attacks. The aim of both is to prevent data packets to reach the destination node and dropping all the traffic.

Keywords: *MANET, AODV, Blackhole Attack, Wormhole Attack, NS2 Network Simulation.*

1. Introduction

MANET is a self- configuring mobile nodes creating a temporary dynamic topology network connected by wireless links with absence of physical fixed infrastructure. Mobile nodes communicate directly and may change speedily and randomly where any node can leave and join freely as a result breaking of communication link is very frequent [1][2][3]. MANETs are used in military, intelligent agriculture, transport systems, disaster avoidance systems and environmental monitoring systems. Due to the proliferation of MANETs applications, security issues are also increasing. MANET has no access point each nodes acts as a router and host to forwards packet to each other independently[4][5][6][7].On other hand, there are many challenges faced MANET due to dynamic topology, distributed operation between nodes, lack of centralization and the limitation of its resources that will affect nodes communication [8][9][10].

Moreover, security issue is very critical in MANETs therefore, data transferring needs to be in secure pattern without any change. Implementation of data encryption enhance the confidentiality in MANETs. All nodes through the network should trust each other and exchange secure messages to prevent any access from unauthorized users [3]. To protect network, authentication mode require in the stage of sharing the packets.

Maintain the security and privacy in MANETs is particularly important. Link communication and messages require to be more secure and confidence

However, Due to the characteristics of MANETs system, the security issues have to be more critical and sensitive. Numerous of attacks can be established in MANETs network and data which share between the nodes may change by the attackers. The reliability of getting message over this network must rise and take in priority for enhancement of security criteria.

Malicious action that leads to bad effects to the system is called “Attack”. Most of the disadvantages of attacking the system is getting sensitive data about the victim and damage the network. In other words, the major objectives of attacking process are breaking security criteria such us availability, integrity and confidentiality of the target network [6].

MANETs improve day by bay to satisfy the frequent developments. For that, there are several security challenges occurs that need to sort out for management goal. Moreover, vehicular networks are depending on wireless technology to execute the functions of mobility [10].

MANETs effect by attack operation unless taking the security policies in priority.

Rest of the paper is organized as follows: in Section 2, gives an overview of related work in AODV routing protocol, Blackhole and Wormhole attacks. For understanding AODV protocol and its works, Section 3 discussed it in brief. In Section 4, Blackhole and wormhole attacks in While Ad-Hoc On demand Distance Vector (AODV) protocol is summarised. While Section 5, covers the Methodology of Blackhole and Wormhole attacks in NS2 environment. Finally, in Section 6 this paper concludes with the result, analysis and impact of these two attacks.

2. Related Work

In MANET, as the nodes can be connected in a dynamic and arbitrary manner, each node has to rely on each other in order to forward packets. They need to use a specific cooperation mechanism that use routing protocols to forward packets from hop to hop before it reaches the destination. The main function of these routing protocols is to find the shortest path between the source and the destination nodes. Routing specifies the technique of how routing table is formed to maintain information about its linking node, new node and neighbours for sending a message from sender to destination [11]. There are three types of routing protocols namely Proactive, Reactive and Hybrid. As example of Proactive routing protocol are Destination Sequenced Distance Vector (DSDV) and Optimal Link State Routing OLSR[12][13]. While Ad-Hoc On demand Distance Vector (AODV) and Dynamic Source Routing Protocol (DSR) are examples of Reactive Protocol[14][15]. Further more example of Proactive routing protocol are Zone Routing Protocol (ZRP) and Zone Based Hierarchical Link State routing protocol (ZHLS) [16][17].

This paper will focus on AODV as is the most routing protocol been widely used for many reasons such as provide quick adaptation to dynamic link conditions, low network

utilization, low processing and memory overhead and determines unicast routes to destinations within the ad hoc network. In addition, it uses destination sequence numbers to ensure loop freedom at all times and avoiding problems of counting to infinity that associated with classical distance vector protocols.

Ad Hoc on Demand Distance Vector (AODV) is a reactive routing protocol improved version of Destination Sequenced Distance Vector (DSDV) .On AODV algorithm routes are created on a demand basis, as opposed of DSDV where its routing table is maintained frequently even there in no Route Request (RREQ). AODV protocol is classified as a pure on demand route , as only the nodes on selected patch are participate and maintain routing table exchanges[11][18] [19]. AODV routing protocol works as the following steps:

Route Discovery, when source node want to send data packet to some node destination and there is not optimal rout Known, in this case source node initializes route discovery process by broadcast RREQ to all neighbours. They keep forward this request until, reach the destination or an intermediate node located with a "fresh enough" route to the destination. AODV uses destination sequence numbers to ensure route is loop free and has recent route information.

Route Replay (RREP), generated by the intermediate nodes that involve in route discovery process as unicast replay to the source node by placing the route record contained in the route request into the route reply. The initiator selects the route that having shortest path and starts sending data packets in its direction.

Route Maintenance, due to the node movements the route-breaking trigger to the neighbour nodes and transmit the route error (RERR) packets to the every active nearby nodes. Then the source node re-initiate route discovery for transmitting the data packets to the destination.

As MANET lack an infrastructure and central controller , it is exposed to a lot of attacks. Attacks in MANET classified to active and passive attacks, which depends on the malicious node behaviour on network. The malicious node use to either read the secret information or change the information. Routing attacks the most vulnerable attack because of the cooperative nature of the nodes and lack of infrastructure for routing. The malicious node(s) can attack MANET using different methods, such as sending fake messages, fake routing information, and fake advertising links to disrupt the routing operations. Examples of these attacks such as link spoofing, flooding attack, wormhole attack, blackhole attack and colluding miss relay attack [20].

Link spoofing Attack:- aims to disconnect links among nodes where a malicious node block link broadcasts of a specific node or a group of nodes. However, in spoofing attack a malicious node broadcast fake route information to disrupt the routing operation[21]. In consequence, the malicious node manipulates the data or routes traffic. For Example in the OLSR protocol, an attacker broadcasts fake link targeting two- hop neighbours. The target nodes select the malicious node to be its MPR (Multiple point replay); the malicious node, thereby, can modify or drop the routing traffic or attack Dos.

Flooding attack:- achieved by either using RREQs or Data flooding .The aim of it is to consume network resources and interrupt the routing set-up to declined the network performance[22]. For example, in AODV protocol, a malicious node sends a huge number of RREQs (Route Request) for none exits destination in a short period. Because there are no replays, the requests will flood the whole network. As a result, all nodes power and bandwidth will be consumed which could lead to service rejection.

Blackhole attack:- a malicious node aim to make other nodes routing data packets through fake rout information as it is an ideal route .Then it drops all packets instead of forwarding them [23]. For example, in AODV protocol, the attacker sends fake RREP (Route Replay) to the source showing a sufficient fresh route. This causes the source node to select this route; thus, all traffic will be routed to the attacker.

Wormhole attack:- it is one of the most aggressive attacks in MANET. In this attack, wormhole nodes create a fake route as it has the shortest path to destination. It use a tunnelling between two or more malicious nodes that are contribute in this attack. The tunnel here is known as a wormhole. For example, in DSR and AODV routing protocol, the attack could prevent the discovery of any routes through the wormhole if there is no defense mechanism in these routing protocols. As a result, they will not be able to discover valid routes [24] .

Colluding MisRelay attack :- occurs when many malicious nodes work in collusion to alter or drop data packets to interrupt routing operation in MANET. This attack is difficult to detect through the conventional methods such as watchdog and pathrater [21]. For example, an attack occurs in OLSR protocol where two malicious nodes exit. One attacker forwards routing packets to avoid reaching destination and the second attacker drops or modifies the routing packets.

This paper examines blackhole and wormhole attacks in AODV routing Protocol. These attacks are described below:

Blackhole attack in AODV :- in this attack, malicious node sends fake route replay as an optimal short route aiming to drops all packets instead of forwarding them. The attacker drops all packet before the route discovery initiator get an acknowledgment from the destination. In AODV, when a source node flood RREQ for a rout discovery to the nearby nodes to find a fresh path to the destination. A Blackhole node send false information in RREP message that it has the greatest sequence number with fresh enough path to the destination. Therefore, source node sends its data packets through the attacker node to the destination supposing it is a true path. Hence, Black hole attacks drops all the data packets [23].

Wormhole attack in AODV: In this attack, wormhole nodes create a fake route as it has the shortest path to destination. It use a tunnelling between two or more malicious nodes that are contribute in this attack. In AODV, when a source node flood RREQ for a rout discovery to the nearby nodes to find a fresh path to the destination. A wormhole node send fake information in RREP message with a high speed that it has the shortest path to the destination. Therefore, source node sends its data packets through the attacker node to the destination supposing it is an optimal path. Wormhole attacks work as peer at different locations forming a channel .When the first malicious node receive the data packets spreads them to another malicious node through tunnelling then, drops them [24][25]. The steps of wormhole function are illustrated in figure 2.

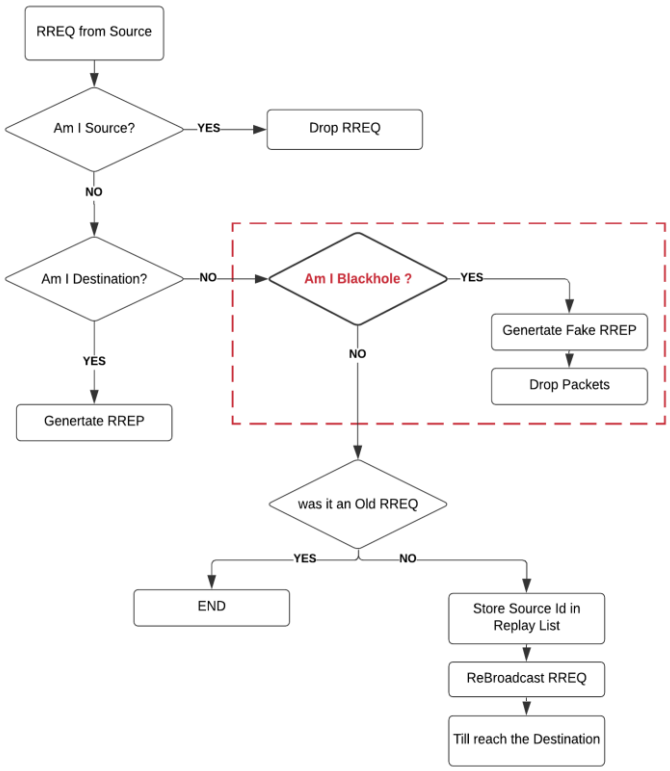

Figure 1. Blackhole in AODV routing protocol

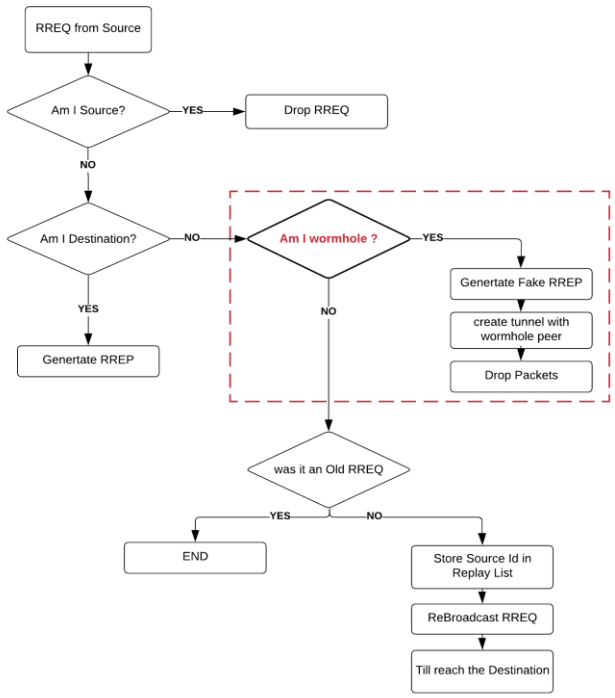

Figure 2. Wormhole in AODV routing protocol

3. Methodology

This paper simulates both Blackhole and Wormhole attacks in MANET and evaluated their impacts. Implement malicious behaviours of both attacks in simulation using Network Simulator version 2 (NS2). NS2 is a software consist of protocols to simulate current network topologies. NS2 does not have any modules to simulate malicious protocols. Therefore, to simulate Blackhole and Wormhole attacks need to do some modification in AODV files for Blackhole attack and MAC files for Wormhole attack.

A. Blackhole attacks Implementation

The files that need to be modified in order to implement and lunch this attack are located in the directory of the NS2 (/ns-allinone-2.35/ns-2.35/AODV) which is mainly to compile and run the AODV routing protocol. First file is AODV.h in which declare a new variable as a malicious agent that define balckhole attacker node. Second file is AODV.cc in which the main modification are applied as follow: In Constructor scope initialize the pervious declared variable in order to distinguish between normal node from black hole node , then in the AODV::command() function identify the black hole node once it participates in the communication. The rest of modification is applied in AODV::AODV() function . In AODV::recvRequest() function generates fake route replies with fake value . While in AODV::rt_resolve() function add few line to drop the received data and prevent sending error message Since, all attackers do not have route to destination, attackers have to disable the send (error). Finally, all ns2 C++ objects have been rebuilt for the above modification to take place.

B. Wormhole attacks Implementation

The implementation of this attack is completely different from Blackhole attack as it works in peer of malicious nodes and create a tunnel. The required files need to be modified are located in the directory of the NS2 (/ns-allinone-2.35/ns-2.35/MAC). First file is ll.h in which a structure been declare with it data elements named “wormhole_peer_struct” and in the protected scope declare a variable as wormhole node. Second file is ll.cc in which initialize wormhole peer list head with values in Constructor. Then, block of code is been added to create wormhole peer nodes with assigning dynamic sector of memory with data sector with condition of if link layer does not allocate memory, as result nodes will not be created. In LL::sendDown(Packet* p) function the unicasting and broadcasting declared with initialization as well as in case of NS_AF_ILINK: add block of code to check next hop for wormhole peer either broadcast or unicast as (physical address) while in case NS_AF_NONE as (IP address) different block of code is added. Furthermore, two block of codes are been added to show the progress of wormhole in two case (broadcast or unicast). The third file is arp.cc in which converting of physical address to logical address code is been added in Address Resolution Protocol (ARP) Table::arprequest part in order to pass this code back through the link layer (ll) will let every peer of wormhole node create tunnel a packet-using broadcast. While in Header Common Access (hdr_cmn), whatever will be hold by ll will be drop (send down). Where llinfor->hold_=0; means no packet will be hold by this node. Finally, all ns2 C++ objects have been rebuild for the above modification to take place.

4. Simulation Results

The performance of the AODV protocols under these two attacks is compared using three performance metrics: packet delivery ratio, average end-to-end delay, and normalized routing load. Packet delivery ratio is the ratio of the data packets delivered to the destinations to the packets generated by the constant bit rate (CBR) sources. The success of a protocol is shown by the performance of delivering packets from source to destination. It is calculated as follows:

$$pdf(\%) = \left\{ \frac{\sum_{m=1}^{n} recvs}{\sum_{m=1}^{n} sends} \right\} \text{x } 100 \qquad (1)$$

Average end-to-end delay of data packets is the total delay experienced by the packet experiences while traveling toward the destination. This metric describes the packet delivery time. A lower end-to-end delay leads to better routing protocol performance. The average e2e delay is computed by,

$$E2E = \frac{\sum_{m=1}^{n} PkTduration}{\sum_{m=1}^{n} recvnum} \qquad (2)$$

Normalized routing load is the number of routing packets transmitted per data packet delivered at the destination. This metric generally evaluates the efficiency of the routing protocol. It is calculated as follows:

$$NRL = \frac{\sum_{m=1}^{n} RPgen}{\sum_{m=1}^{n} recvs} \qquad (3)$$

Table 1 shows the simulation scenario used for NS2 simulation. It consists of the generation of two input files to NS-2. The first file is a scenario file that contains the movement pattern of the nodes and the second file is a communication file that contains the traffic in the network. These two files as input for the simulation and the result of this is a trace file generated as an output of the simulation.
This scenario is generated by a Random waypoint model Where nodes are randomly distributed with uniform speed The numbers of nodes tested in a terrain area of 1300m x 500m are 50 nodes included the malicious nodes varied form none to 10 malicious nodes. While it includes no pause time between changes in destination and speed as well as 5 maximum number of connections allowable.

Table 1. Simulation Scenario

Parameter	*Value*
Protocols	AODV
No. of Nodes	50
Simulation Time	900 ms
Traffic Type	CBR
Mobility Model	Random Waypoint
Simulation Area	1500m X 300m
Maximum Speed	10ms
Packet size (bytes)	500
Pause time	0
Number of Connections	5

Figure 3 shows the procedure chart to execute simulation on NS2.

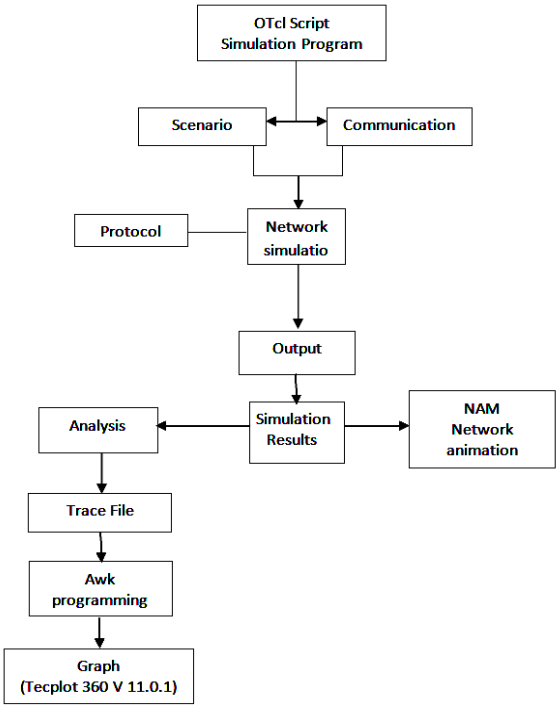

Figure 3. The procedure chart to execute simulation on NS2.

Using outputs from awk script following graphs and results are generated .These graphs show the vulnerability of AODV protocol against blackhole and wormhole attacks , evaluate the effect of them and examine the performance of network simulator under these attacks using PDF, NRL and E2E performance parameters factors with varied number of malicious nodes.
Figure 4 illustrates the impact of blackhole and wormhole attacks on PDF. Blackhole attack has higher impact than wormhole attack as blackhole malicious node aim to obtain the rout and drops packets directly while wormhole malicious node has to find a worm peer to create tunnel mean while configuring tunneling, due to node movement link might be broken before drops occurs. As result, blackhole attack drops packet more than wormhole attack.

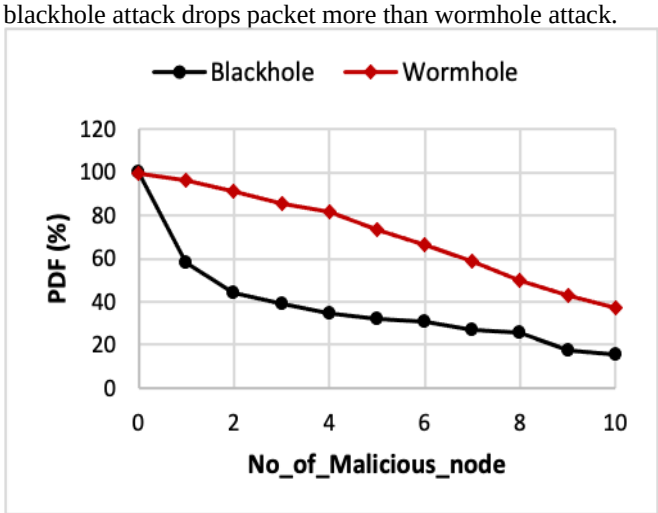

Figure 4. Impact of Black hole and Worm hole Attack on Packet Delivery Ratio.

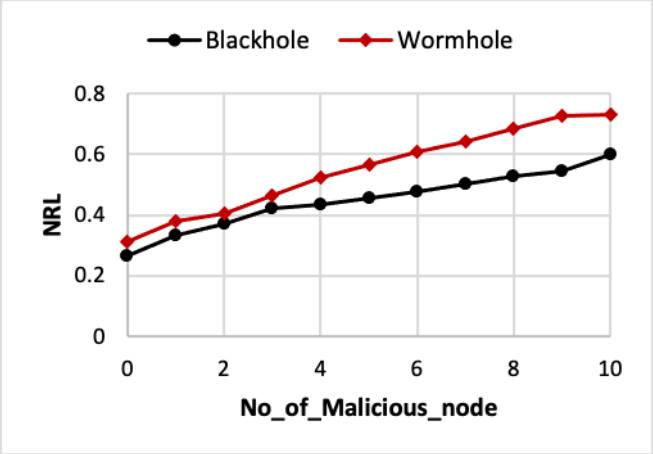

Figure 5. Impact of Black hole and Wormhole Attack on Normalization.

Figure 5 illustrates the impact of blackhole and wormhole attacks on NRL performance parameter. Wormhole has high impact compared to blackhole because when the number of malicious nodes increased the network need to recover and find the optimal route to destination so more control packages get increased as a result NRL increase but there is slightly difference between blackhole and wormhole as shown while blackhole shows better normalization than wormhole.

Simulation results in figure 6 shows that blackhole attack has less end to end delay than wormhole attack as the number of malicious nodes increased. It illustrates that blackhole attacks has less impact than wormhole as wormhole has higher effect on AODV protocol performance due of the high numbers of control packages.

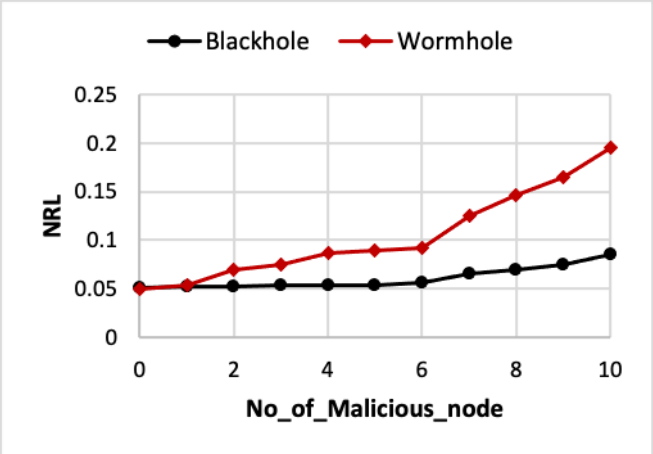

Figure 6. Impact of Black hole and Wormhole Attack on End-to-End delay

5. Conclusion

This paper analyses the network performance parameters of blackhole and wormhole attacks against AODV routing protocol with varied number of malicious nodes . As in case of multicast network AODV routing protocol tested under these attacks because it is most routing protocol been widely used and many networks communication suffer from these attack result on packets loss. Blackhole attack has higher impacts compared to wormhole attacks as its has higher PDF. But network perform better under blackhole attack as it has less NRL and End-2-End delay compared to wormhole attack.

References

[1] M. N. Alslaim, H. A. Alaqel, and S. S. Zaghloul, “A comparative study of MANET routing protocols,” 2014 3rd Int. Conf. e-Technologies Networks Dev. ICeND 2014, pp. 178–182, 2014.

[2] N. Gupta and R. Gupta, “Routing protocols in Mobile Ad-Hoc Networks: An overview,” Int. Conf. "Emerging Trends Robot. Commun. Technol. INTERACT-2010, pp. 173–177, 2010.

[3] N. Raj, P. Bharti, and S. Thakur, “Vulnerabilities, challenges and threats in securing mobile ad-hoc network,” Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015, pp. 771–775, 2015.

[4] A. Srivastava, A. Mishra, B. Upadhyay, and A. K. Yadav, “Survey and overview of Mobile Ad-Hoc Network routing protocols,” 2014 Int. Conf. Adv. Eng. Technol. Res. ICAETR 2014, pp. 0–5, 2014.

[5] S. Habib, S. Saleem, and K. M. Saqib, “Review on MANET routing protocols and challenges,” Proceeding - 2013 IEEE Student Conf. Res. Dev. SCOReD 2013, no. December, pp. 529–533, 2015.

[6] G. S. Dhillon, “Available Online at www.ijarcs.info Vulnerabilities & Attacks in Mobile Adhoc Networks (MANET),” vol. 8, no. 4, pp. 2015–2017, 2017.

[7] A. Kaid, S. Ali, and U. V Kulkarni, “Characteristics , Applications and Challenges in Mobile Ad-Hoc Networks (MANET): Overview,” vol. 3, no. 12, pp. 6–12, 2015.

[8] D. Ahmed and O. Khalifa, “An overview of MANETs: applications, characteristics, challenges and recent issues,” Ijeat, vol. 3, no. 4, p. 128, 2017.

[9] G. S. Dhillon, “Available Online at www.ijarcs.info Vulnerabilities & Attacks in Mobile Adhoc Networks (MANET),” vol. 8, no. 4, pp. 2015–2017, 2017.

[10] A. Kaid, S. Ali, and U. V Kulkarni, “Characteristics , Applications and Challenges in Mobile Ad-Hoc Networks (MANET): Overview,” vol. 3, no. 12, pp. 6–12, 2015.

[11] M. N. Abdulleh, S. Yussof, and H. S. Jassim, “Comparative Study of Proactive , Reactive and Geographical MANET Routing Protocols,” no. May, pp. 125–137, 2015.

[12] V. Bhatt and S. Kumar, “Study and Literature or Research Survey of Routing Protocols and Routing Attacks in MANET with Different Security Technique in Cryptography for Network Security,” Int. J. Futur. Revolut. Comput. Sci. Commun. Eng., vol. 4, no. 4, pp. 839–845, 2018.

[13] M. Education, “An application , challenges and routing protocol in Mobile Ad-Hoc Network,” vol. 2, no. 5, 2015.

[14] N. Gupta and R. Gupta, “Routing protocols in Mobile Ad-Hoc Networks: An overview,” Int. Conf. "Emerging Trends Robot. Commun. Technol. INTERACT-2010, pp. 173–177, 2010.

[15] S. Wali, S. I. Ullah, A. W. U. Khan, and A. Salam, "A Comprehensive Study on Reactive and Proactive Routing Protocols under different performance Metric," vol. 1, no. 2, 2018.

[16] A. Zain, H. El-khobby, H. M. Abd Elkader, and M. Abdelnaby, "MANETs performance analysis with dos attack at different routing protocols," Int. J. Eng. Technol., vol. 4, no. 2, p. 390, 2015.

[17] K. Raheja and S. K. Maakar, "A Survey on Different Hybrid Routing Protocols of MANET," Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 5, pp. 5512–5516, 2014.

[18] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016, pp. 525–530, 2017.

[19] S. Habib, S. Saleem, and K. M. Saqib, "Review on MANET routing protocols and challenges," Proceeding - 2013 IEEE Student Conf. Res. Dev. SCOReD 2013, no. December, pp. 529–533, 2015.

[20] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," 2017 Int. Symp. Wirel. Syst. Networks, ISWSN 2017, vol. 2018–Janua, pp. 1–4, 2018.

[21] M. Ngadi, R. Khokhar, and S. Mandala, "A review current routing attacks in mobile ad-hoc networks," Int. J. …, no. 2, pp. 18–29, 2008.

[22] K. Gupta and P. K. Mittal, "An Overview of Security in MANET," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 6, pp. 151–156, 2017.

[23] A. Tiwari and P. N. Verma, "Comparative Study of Routing Attacks and Discuss the Solutions to Mitigate Black Hole and Flooding Attacks in AODV Based MANET," vol. 3, no. 2, pp. 248–253, 2014.

[24] M. Sadeghi and S. Yahya, "Analysis of Wormhole attack on MANETs using different MANET routing protocols," ICUFN 2012 - 4th Int. Conf. Ubiquitous Futur. Networks, Final Progr., pp. 301–305, 2012.

[25] Reddy, K. Ganesh, and P. Santhi Thilagam. "Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks." International Journal of Communication Networks and Information Security 12.2 (2020): 221-226.