iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39467

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Countering of Black Hole Attack on Manet with AODV Protocol

Gurwinder Singh[1], Dr. Ashish Oberoi[2], Prof. Jasdeep Singh[3]
[1]*Department of Civil Engineering, Rimt University, Opposite Floating Restaurant, Sirhind Side, Mandi Gobindgarh-147301, Punjab (INDIA)*

Abstract: ***Security in mobile ad-hoc network (MANET) is the most serious issue impacting performance of network. In general, routing methods is one of the complicated and exciting analysis places. In black hole attack, a harmful node uses its routing technique to be able to promote itself for having the quickest direction to the place node or to the bundle it wants to identify. In this research, performance of one of the most efficient solutions for preventing single black hole attack in MANET using AODV routing protocol will be investigated in terms of packet delivery ratio, packet loss percentage, average end-to-end delay, and route request overhead. This chapter describes the introduction, background of the study, research objectives and questions, the scope of the study and its primary objectives.***

I. INTRODUCTION

As the importance of computers in our daily life increases it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting to the internet, reading and sending E-mail messages, changing information in a meeting and so on. In Latin, ad hoc means “for this”, further meaning “for this purpose only”. It is a good and emblematic description of the idea why ad hoc networks are needed. They can be set up anywhere without any need for external infrastructure (like wires or base stations). They are often mobile and that’s why a term MANET is often used when talking about Mobile Ad hoc NETworks. MANET’s are often defined as follows” A “mobile ad hoc network” (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network’s wireless topology may change rapidly and unpredictably, such a network may operate in a standalone fashion, or may be connected to the larger internet. Simple Ad-hoc Network The strength of the connection can change rapidly in time or even disappear completely. Nodes can appear, disappear and re-appear as the time goes on and all the time the network connections should work between the nodes that are part of it. As one can easily imagine, the situation in ad hoc networks with respect to ensuring connectivity and robustness is much more demanding than in the wired case. Ad hoc networks are networks which are not connected to any static (i.e. wired) infrastructure. An ad hoc network is a LAN or other small network, especially one with wireless connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network. The ad hoc network is a communication network without a pre-exist network infrastructure. In cellular networks, there is a network infrastructure represented by the base-stations, Radio network controllers, etc. In ad hoc networks every communication terminal (or radio terminal RT) communicates with its partner to perform peer to peer communication. If the required RT is not a neighbour to the initiated call RT (outside the coverage area of the RT), then the other intermediate RT’s are used to perform the communication link. This is called multi-hop peer to peer communication. This collaboration between the RT’s is very important in the ad hoc networks. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals (i.e. the communication terminals should be independent and highly cooperative).

A mobile ad hoc network (MANET) is a self-configuring network of mobile nodes. It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. Wireless ad hoc network can be built up where there is no support of wireless access or wired backbone is not feasible. All network services of ad hoc network are configured and created on the fly. Thus, it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness. Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication, link the node should be capable enough to identify another node. As a result, node needs to provide his/her identity as well as associated credentials to another node.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

However, delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore, it is essential to provide security architecture to secure ad hoc networking. We found that many of the presently existing attacks have some common features and have been categorized into different attacks based on their minor differences. So hereby we are trying to categorize them into two broad categories: DATA traffic attacks and CONTROL traffic attacks. This will help in future designing of security measures.

1.1 Ad-hoc On-demand Distance Vector (AODV) AODV is a kind of reactive protocols. It methodology is hop-to-hop routing. The node establishes the Route Request (RREQ) if it wants to know the route to a particular destination. Then the intermediate nodes forward the route request and at the same time, these intermediate nodes create a reverse route to the destination. When the node receives the request that has the route to the destination, it establishes a Route Reply (RREP) which includes numeral of hops which are required to arrive the destination. Each node that cooperates in sending this reply to the source node, it creates a forward route to the destination. This route that has been established from source to destination is a hop-by-hop case.

A. Dynamic Source Routing (DSR)

DSR is a reactive or on-demand routing protocol. This protocol has been designed to reduce the bandwidth wasted via the control packets in wireless networks and that via deleting the periodic table-update messages required in the table-driven approach. In DSR protocol, there is no need for network infrastructure or administration, due to these networks fully self configured and organized. The source routing is a method which the source packet defines the complete sequence of nodes through which to forward the data packets. The source routing does not need to keep the routing information via the intermediate hops. Figure 3 shows the advantages and disadvantages of DSR protocol.

B. Destination Sequenced Distance Vector (DSDV)

DSDV is one of the most widely known proactive or table-driven routing protocols for MANETs. The routing algorithm of DSDV is depended on the numeral of hops to arrive at the destination node. To transmit the data packets among the nodes in the network, DSDV protocol utilizing routing tables which are stored in every node. DSDV protocol has three major characteristics which are: decreasing the high routing overhead, solve the “count to infinity” problem and avert the loops. Each mobile node contains a table of routing information which includes all the routes to the destinations and another information.

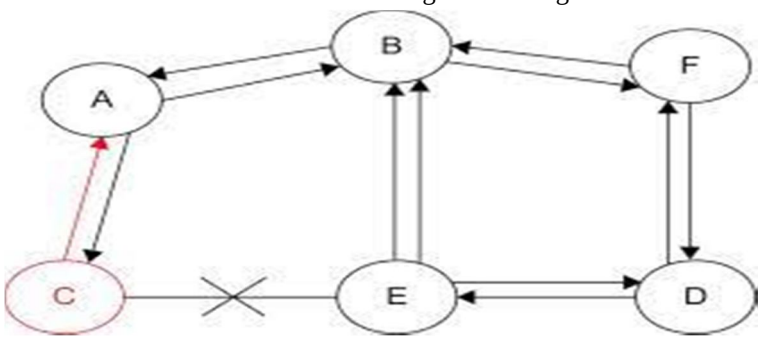
C. Black Hole Attack

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components.

Few strategies to mitigate the problem:

1) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found.

2) Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbours and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

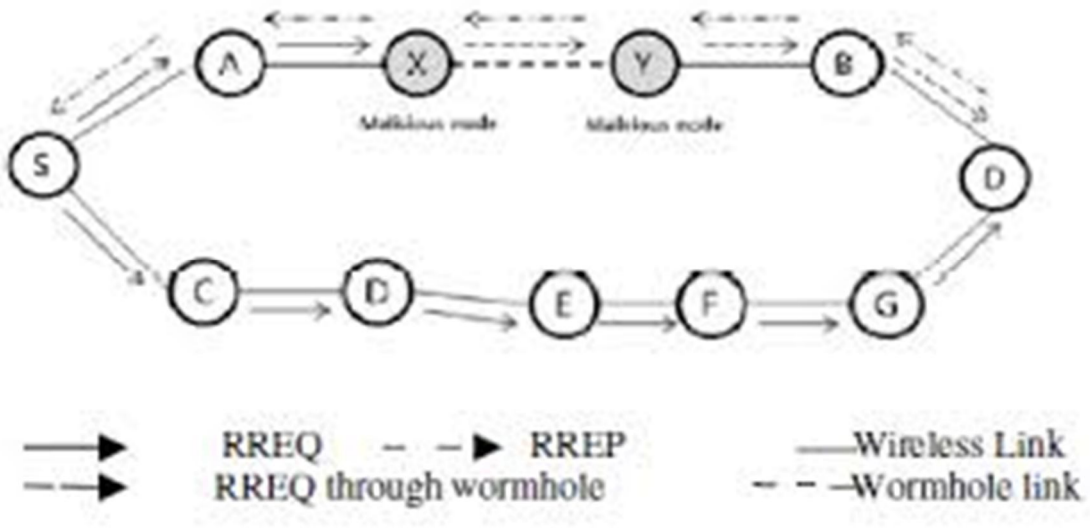


3.1 Black hole attack

©IJRASET: All Rights are Reserved

D. Worm Hole

Connects two distant points in space via a shortcut route. In the same way in MANET also one or more attacking node can disrupt routing by short-circuiting the network, thereby disrupting usual flow of packets. If this link becomes the lowest cost path to the destination, then these malicious nodes will always be chosen while sending packets to that destination. The attacking node then can either monitor the traffic or can even disrupt the flow (via one of the DATA traffic attacks). Wormhole attack can be done with single node also but generally two or more malicious node connects via a wormhole-link. In figure 5, Node X and Y performing wormhole attack.



3.2 Worm hole Attack

II. LITRATURE SURVEY

Sureka.N1, Prof. S. Chandra Sekaran proposed resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase. The wireless Adhoc sensor network and routing data in them is vulnerable to certain attacks. So, we must ensure a secure and authenticated data transmission process. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack draining of node life from wireless adhoc sensor networks. Adhoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications.

Harsha.N1, Rashmi.S proposed an approach to detect and prevent the vampire attack in MANET. Ad-hoc low-power wireless networks are the most promising research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of service at the routing or medium access control levels. Earlier, the resource depletion attacks are considered only as a routing problem, very recently these are classified in to a new group called "vampire attacks". Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing .It is clear that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant International Journal For Technological Research In Engineering Volume 4, Issue 10, June-2017 ISSN (Online): 2347 - 4718 www.ijtre.com Copyright 2017.All rights reserved. 2073 messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. Sumit Agrawal, Shilpa Jaiswal proposed a Secure Ad-hoc On-Demand Distance Vector routing protocol (SAODV) to endeavour our all efforts into a common place. So, the emphasis is to develop a scheme for the measure of these network worms and blackhole attacks to eliminate occurrences of communication hazards from intermediate and surrounding threads. the full study to eliminate thread of black hole attacks in MANET". We also address to the solution against the threat of

black hole attack in MANET. In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. So, to rectify the possibility of occurrence of black hole attack we are proposing a technique to identify attack and a solution to discover a safe route for secure transmission. The need of wireless network is to enforce participating nodes to forward packets to other nodes to foster secure and reliable communication. Although there is presence of vulnerable nodes that can be associated with malicious nodes and can harm networks.

The varieties of these malicious nodes are vulnerable to nodes which are either compromised or falsely guided by vulnerable nodes. Malicious nodes can easily tamper the participating nodes in the networks. In mobile ad hoc network these attacks shown their significance in the terms of network worms which can attack, alter or modify the root definitions of network across all administrative and participating domains.

Saritha Reddy Venna1, Ramesh Babu Inampudi proposed vulnerabilities and various kinds of security attacks in MANETs the recent and rapid advancements in the technology and the distinct features of MANETs have made the use of MANETs more prevalent. With the ever-increasing applications, the weakness of these networks against a variety of attacks has been unveiled. MANETs doesn't have clear and efficient mechanisms to detect or prevent the attacks, so attacker node can easily interrupt and destroy the whole system or may take control over the information being transmitted in the network. Attackers introduce various kinds of attacks and every attack has its own degree of impact on the network. Security is a major concern in MANETs because of its intrinsic vulnerabilities.

Each mobile node can work either as a host or as a router. There is no necessity of fixed infrastructure and these mobile nodes organize themselves in an arbitrary fashion to form a temporary network with dynamically changing topology. Nodes within each other's wireless transmission ranges can communicate directly but nodes outside each other's range have to depend on neighbouring nodes to relay messages.

Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba proposed different mechanisms of collaboration and defence in collaborative security. We systematically investigate numerous use cases of collaborative security by covering six types of security systems.

Aspects of these systems are thoroughly studied, including their technologies, standards, frameworks, strengths and weaknesses. We then present a comprehensive study with respect to their analysis target, timeliness of analysis, architecture, network infrastructure, initiative, shared information and interoperability. We highlight five important topics in collaborative security, and identify challenges and possible directions for future research.

Our work contributes the following to the existing research on collaborative security with the goal of helping to make collaborative security systems more resilient and efficient. Security is oftentimes centrally managed. An alternative trend of using collaboration in order to improve security has gained momentum over the past few years. Collaborative security is an abstract concept that applies to a wide variety of systems, and has been used to solve security issues inherent in distributed environments. Thus far, collaboration has been used in many domains such as intrusion detection, spam filtering, botnet resistance, and vulnerability detection.

III. PROBLEM STATEMENT

A. Problem Statement

1) There are many attacks in MANET. But Sinkhole Attack and black hole attack is a special type of Attack.

2) Sink Hole alters the data packet or drops the packet silently.

3) So we implement Sinkhole Attack and Black hole attack on MANET to check the Performance of the network.

4) We check that how much network Performance degrade when we apply Sink Hole and black hole attack on the Network.

IV. OBJECTIVE

A. To Study reactive routing protocol AODV and black hole attack in MANET.

B. To Implement the different simulation scenario's of network using ns2 simulator.

C. To analyze the performance of AODV with and without black hole attack using different scenario's by varying number of nodes in the network.

D. To Compare the impact of black hole attack on the performance of AODV protocol in terms of throughput, packet delivery ratio, end-to-end delay and load.

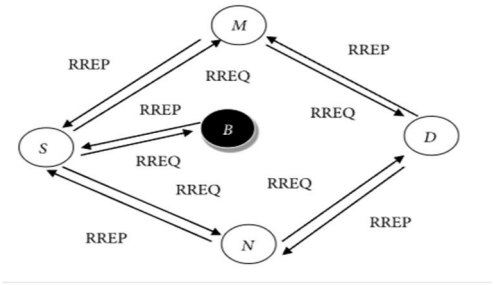
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

V. IMPLEMENTATION

A. *Methodology*

The Implementation is divided into stages and that are:

1) *In Stage1:* We will gather the information and generate the network scenario.
2) *In Stage2:* We will initialize the number of nodes which are required in protocols. Than we will implement protocol system. In that nodes we have to identify the route from where they have to send data.
3) *In Stage 3:*After initialize the nodes we will take AODV protocols and implement these protocols on node.
4) *In Stage 4:* After implementation we will compare the performances of MANET network with & without Black Hole Attack in AODV Protocol.



5.1 Black hole scenario

B. *Tools*

Tools used for the research work are NS2.

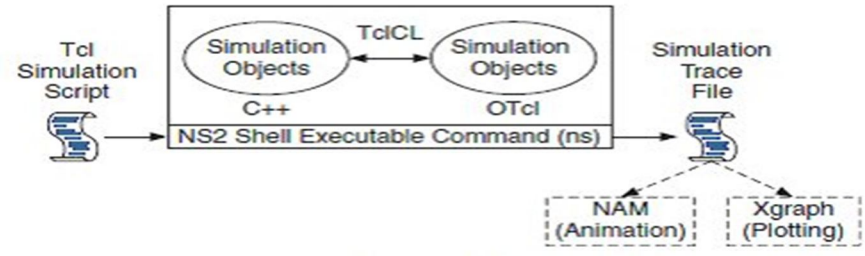
Network Simulator 2 (NS2): Features & Basic Architecture Of NS2

1) *What is NS2:* NS2 stands for Network Simulator Version 2. It is an open-source event-driven simulator designed specifically for research in computer communication networks.
2) *Features of NS2*

a) It is a discrete event simulator for networking research.
b) It provides substantial support to simulate bunch of protocols like TCP, FTP, UDP, https and DSR.
c) It simulates wired and wireless network.
d) It is primarily Unix based.
e) Uses TCL as its scripting language.
f) Otcl: Object oriented support
g) Tclcl: C++ and otcl linkage
h) Discrete event scheduler

C. *Basic Architecture*

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and the OTcl are linked together using TclCL



5.2 Basic architecture of NS

ALGORITHM 1

Step 1: Variable (attacker) declaration

We declare a variable malicious as Boolean within the code aodv.cc, and aodv.h, firstly modifying the code in aodv.h file as below:

Boolean malicious; // or BH

Step 2: Variable (attacker) initialization

We initialize the attacker variable as a false within the constructor of aodv.cc.

Step 3: The normal node is a black_hole (BH), what's happening to the malicious or attacker node value inside some block of code in aodv.cc

file command () function if (argc ==2)

add some lines of code and replace it as the below code

```
if (strcasecmp (argv[1], "black_hole") == 0)
{
attacker = true;
return TCL_OK;
}
```

Step 4: The attacker node is true what will be?

```
if (attacker == true) {
   printf ("Packets are dropped index of node and number of packets %d is as %d \n",
   index, t_count++);
   drop (p,DROP_RTR_ROUTE_LOOP); //dropped all packet based on this function
}
```

After this completion of work, open the command prompt and go to the ~ns-2.35/ then finally run the make command

$ make

If there are no mistakes in the above technique of packets dropped, your compilation and execution will be successful.

Step 5: Finally, we go running Tool Command Language (TCL) file with AODV protocol, with Attacker (BH) modified code and normal code, then comparing total experimental outcomes.

$ ns AODV.tcl

VI. RESULT AND DISCUSSION

1) The End to End delay for AODV and AODV with Black hole attack on the network is shown in figure.

It has shown that initially delay is greater in AODV as comparison to B-AODV due to instant optimal route information sent by malicious node (acting as black hole attacker node) to the sender that will attract to immediately starts sending packets over it.

By the time, as packet doesn't reach to its intended destination, which will result in increasing the e2e delay, as shown in figure.

On the other hand, in AODV, once route generation process completes, the e2e delay is reduced, which exhibits to greater performance

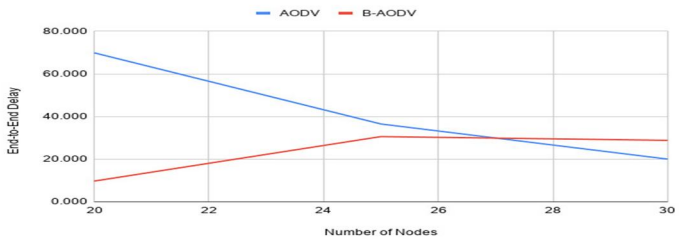
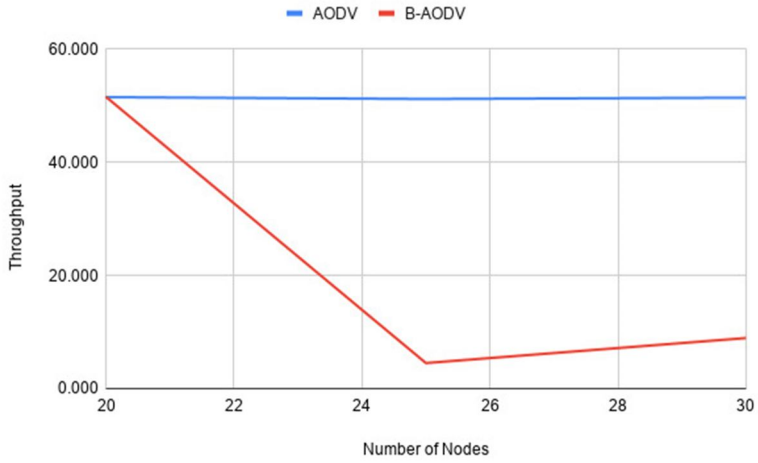


Fig 6.1 End to End delay

Nodes	AODV	B-AODV
20	69.88	9.72
25	36.51	30.60
30	20.04	28.83

Table 6.1 End to End delay

2) Throughput for AODV and AODV with Black hole attack on the network is shown in figure.
Throughput is the average no. of packets sent in per unit time, which is measured in kbps.
It can be seen throughput during black hole attack is dropped due to packets not reaches to its intended destination which will degrade the overall performance of the network.
The PDR reaches to minimum level when no. of nodes participate in a network communication will be 24-26.



6.2 Throughput

Nodes	AODV	B-AODV
20	51.53	51.6
25	5.1.21	4.52
30	51.44	8.94

Table 6.2 Throughput

3) Packet Delivery ratio is rate of packet sent by sender node and packet received to the intended destination successfully.
It is clear from the given graph (gnu plot graph) here, as shown in figure, that rate of success rate of recipient of packets remains increased and consistent, as comparison to AODV with Black hole attack, where dropping of packets are frequently happens.

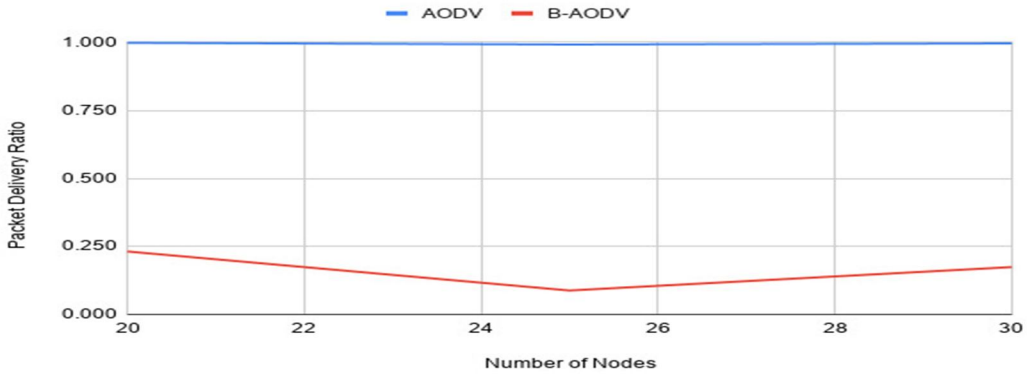


Fig 6.3 Packet Delivery Ratio

Nodes	AODV	B-AODV
20	0.998	0.23
25	0.99	0.08
30	0.99	0.17

Table 6.3 Packet Delivery Ratio

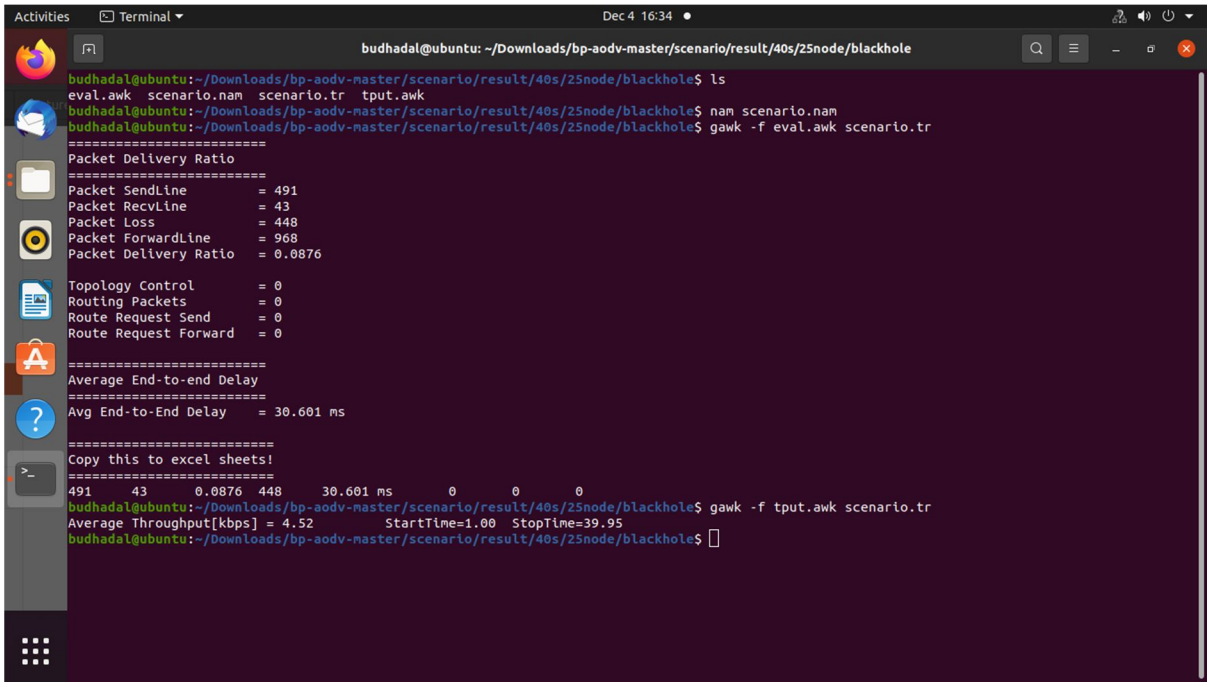


Fig 6.4 Linux Terminal

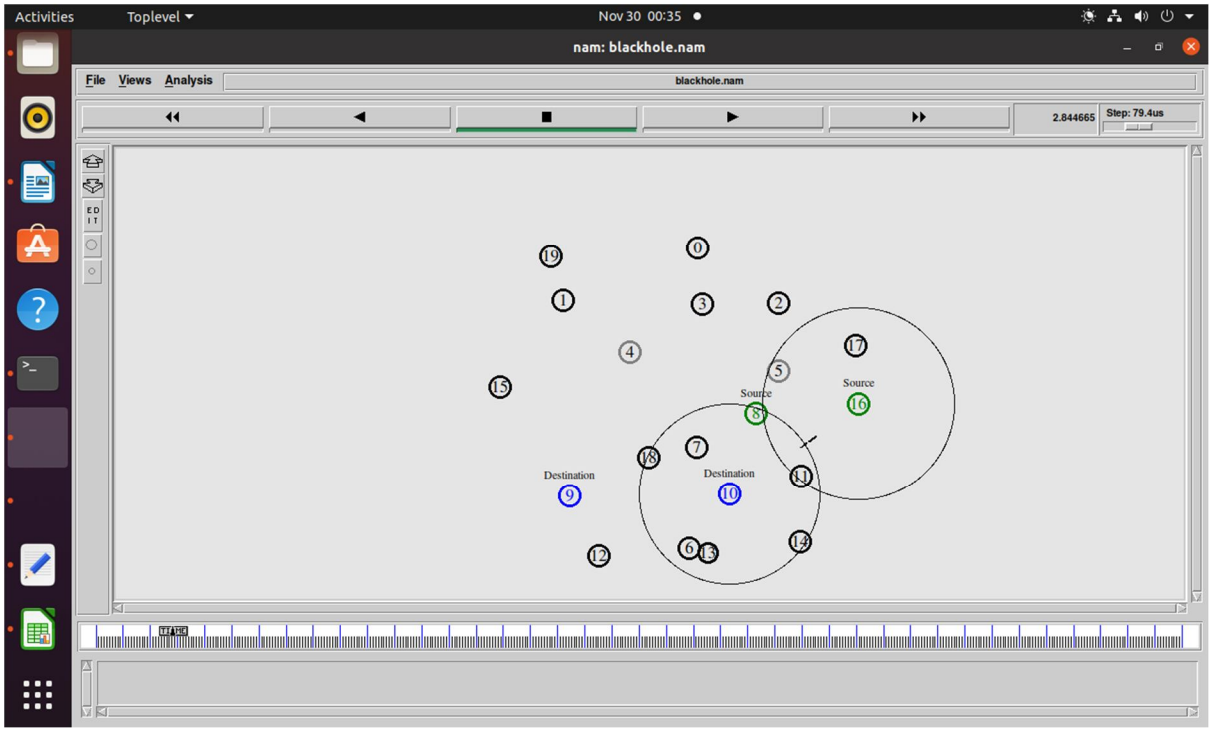


Fig 6.5 Perform Attack

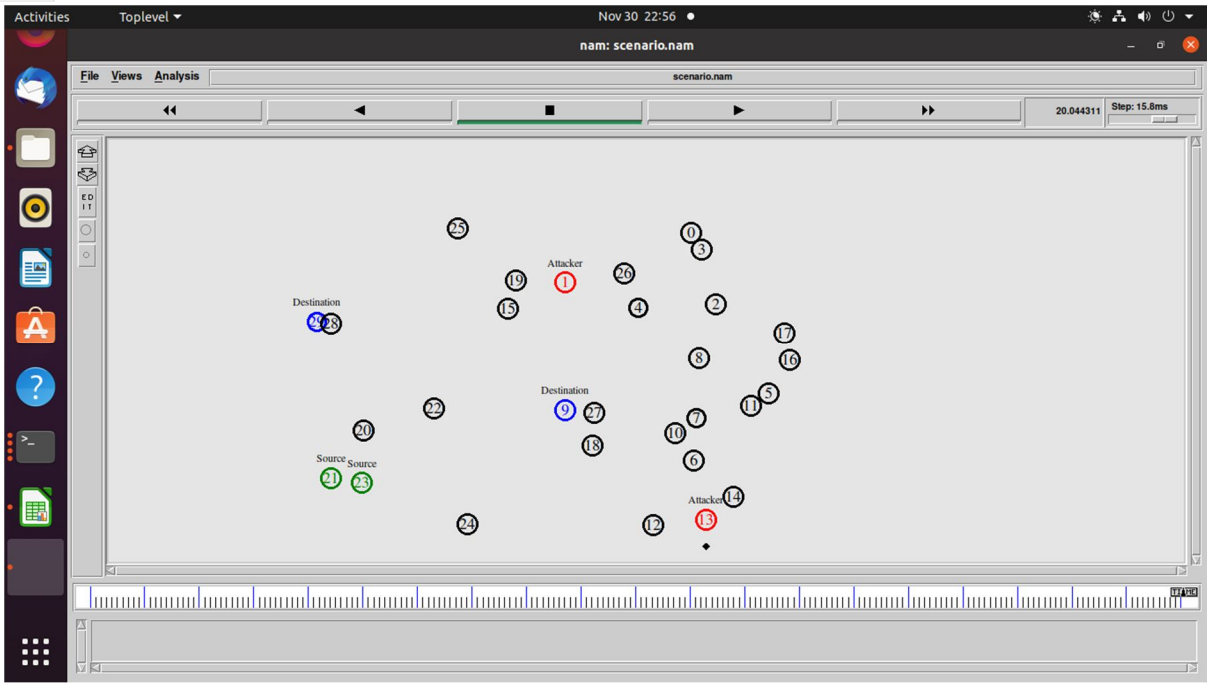


Fig 6.6 Attack on Manets using Black hole

VII. CONCLUSION

A. B-AODV hampers the network performance in terms of dropping the packets by increasing e2e delay and increased load.

B. Wrong route acquisition happens due to frequent false reply packets whenever sender requests for optimal path selection by flooding the RREQ packets.

C. Black hole attacks also serve as a basis for other attacks such as eavesdropping, identity theft etc.

VIII. FUTURE SCOPE

A. In future a more improved mechanisms should be developed to detect & prevent such attacks.

B. This work will also implement to analyse the impact on performance of other reactive routing protocol such as AODV.

REFERENCES

[1] I. Mohd Zaki and H. Rosilah, "The implementation of Internet of Things using test bed in the UKMnet environment," Asia-Pacific Journal of Information Technology and Multimedia, vol. 8, no. 2, pp. 1–17, 2019.

[2] Z. Ismail and R. Hassan, "A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET," in in the 17th Asia Pacific Conference on Communications, IEEE, 2011.

[3] T. Salam and M. S. Hossen, "Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network," Wireless Personal Communications, vol. 113, no. 1, pp. 189–222, 2020.

[4] M. S. Hossen, "DTN routing protocols on two distinct geographical regions in an opportunistic network: an analysis," Wireless Personal Communications, vol. 108, no. 2, pp. 839–851, 2019.

[5] M. Singh, C. Kumar, and P. Nath, "Challenges and protocols for P2P applications in multi-hop wireless networks," in in 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), pp. 310–316, IEEE, 2018.

[6] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: architectures, advances and challenges," Ad Hoc Networks, vol. 55, pp. 143–152, 2017.

[7] C. S. R. Murthy, Ad Hoc Wireless Networks: Architestures and Protocols, Pearson Education India, 2004.

[8] S. M. Adam and R. Hassan, "Delay aware reactive routing protocols for QoS in MANETs: a review," Journal of applied research and technology, vol. 11, no. 6, pp. 844–850, 2013. S. Malathy, V. Porkodi, A. Sampathkumar et al., "An optimal network coding-based backpressure routing approach for massive IoT network," Wireless Networks, vol. 26, no. 5, pp. 3657–3674, 2020

[9] H. M. Haglan, S. A. Mostafa, N. Z. M. Safar et al., "Analyzing the impact of the number of nodes on the performance of the routing protocols in MANET environment," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 1, pp. 434–440, 2020.

[10] S. Yan and Y. Chung, "Improved ad hoc on-demand distance vector routing (AODV) protocol based on blockchain node detection in ad hoc networks," International Journal of Internet, Broadcasting and Communication, vol. 12, no. 3, pp. 46–55, 2020.

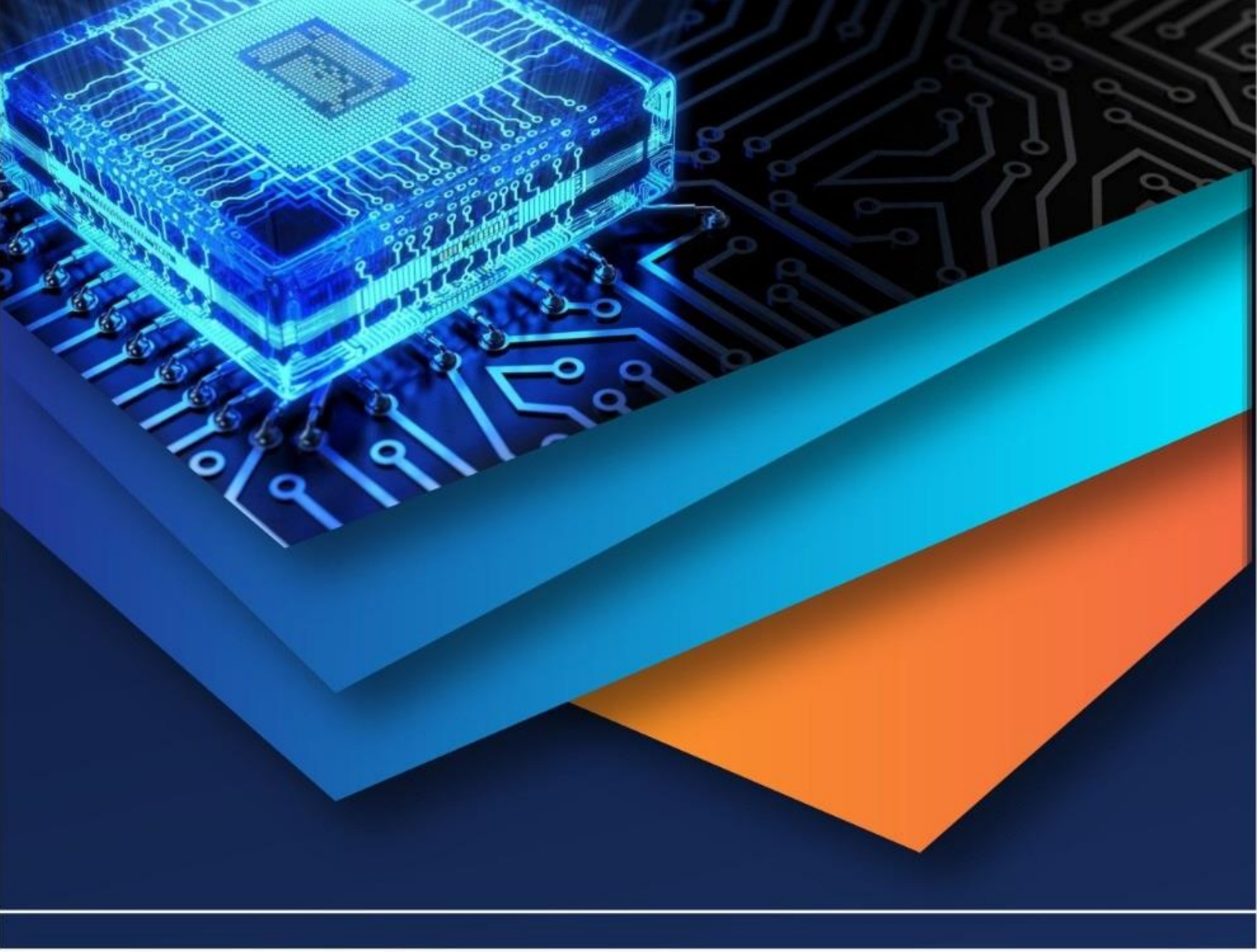
[11] R. K. Mohapatra, S. Samantaray, A. Sahoo et al., "Performance analysis of reactive routing protocols in MANET under CBR traffic using NS2," in in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 352–356, IEEE, 2018.

[12] A. K. Biswas and M. Dasgupta, "AODV-DSR hybrid reactive routing protocol and its generalization for mobile ad-hoc networks," in in 2019 3rd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), pp. 1–5, IEEE, 2019.
[13] V. Sharma, B. Alam, and M. Doja, "An improvement in DSR routing protocol of MANETs using ANFIS," in in Applications of Artificial Intelligence Techniques in Engineering, pp. 569–576, Springer, 2019.
[14] K. L. Arega, G. Raga, and R. Bareto, "Survey on performance analysis of AODV, DSR and DSDV in MANET," Computer Engineering and Intelligent Systems, vol. 11, no. 3, pp. 23–32, 2020.
[15] F. T. AL-Dhief, N. Sabri, M. S. Salim, S. Fouad, and S. A. Aljunid, "MANET routing protocols evaluation: AODV, DSR and DSDV perspective," in in MATEC Web of Conferences, vol. 150, p. 06024, EDP Sciences, 2018.
[16] A. Kulkarni, R. Bukate, and S. Nanaware, "Study of various attacks and routing protocols in MANETS," in in 2018 International Conference on Information, Communication, Engineering and Technology (ICICET), pp. 1–3, IEEE, 2018.
[17] A. M. Fahad and R. C. Muniyandi, "Harmony search algorithm to prevent malicious nodes in mobile ad hoc networks (MANETs)," Information Technology Journal, vol. 15, no. 3, pp. 84–90, 2016.
[18] Z. Pooranian, A. Barati, and A. Movaghar, "Queen-bee algorithm for energy efficient clusters in wireless sensor networks," World Academy of Science, Engineering and Technology, vol. 73, pp. 1080–1083, 2011.
[19] S. H. H. Nazhad, M. Shojafar, S. Shamshirband, and M. Conti, "An efficient routing protocol for the QoS support of large-scale MANETs," International Journal of Communication Systems, vol. 31, no. 1, article e3384, 2018.
[20] M. S. Pathan, J. He, N. Zhu, Z. Ali, M. Qasim, and A. Azmat, "An efficient scheme for detection and prevention of black hole attacks in AODV-based MANETs," International Journal of Advanced Computer Science and Applications, vol. 10, no. 1, pp. 243–251, 2019.
[21] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: a secure and trust-based approach to mitigate blackhole attack on AODV based MANET," in in 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1278–1282, IEEE, 2017.
[22] G. K. Wadhwani, S. K. Khatri, and S. K. Mutto, "Trust framework for attack resilience in MANET using AODV," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 1, pp. 209–220, 2020.
[23] S. El Jay and A. Hasbi, "Security in mobile ad hoc networks (MANETs) and WSNs (wireless sensor networks)," International Journal of Computer Science and Network Security (IJCSNS), vol. 16, no. 9, p. 118, 2016.
[24] M. Y. Thanoun and A. M. Aleesa, "Routing, significant and applications of mobile ad-hoc wireless sensor networks," Journal of Computational and Theoretical Nanoscience, vol. 17, no. 2, pp. 850–854, 2020.
[25] V. Tilwari, M. D. N. Hindia, K. Dimyati, F. Qamar, and M. S. A. Talip, "Contention window and residual battery aware multipath routing schemes in mobile ad-hoc networks," International Journal of Technology, vol. 10, no. 7, pp. 1376–1384, 2019.
[26] V. L. Narayana and C. Bharathi, "Identity based cryptography for mobile ad hoc networks," Journal of Theoretical and Applied Information Technology, vol. 95, no. 5, p. 1173, 2017.
[27] M. Rath and B. K. Pattanayak, "Security protocol with IDS framework using mobile agent in robotic MANET," International Journal of Information Security and Privacy, vol. 13, no. 1, pp. 46–58, 2019.
[28] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks," International Journal of Soft Computing and Networking, vol. 1, no. 1, pp. 17–34, 2016.
[29] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, "Fuzzy based intrusion detection systems in MANET," Procedia Computer Science, vol. 50, pp. 109–114, 2015.
[30] J. Manoranjini, A. Chandrasekar, and S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework," Automatika, vol. 60, no. 3, pp. 274–284, 2019.
[31] Y. M. Khamayseh, S. A. Aljawarneh, and A. E. Asaad, "Ensuring survivability against black hole attacks in MANETS for preserving energy efficiency," Sustainable Computing: Informatics and Systems, vol. 18, pp. 90–100, 2018.
[32] G. Usha, M. R. Babu, and S. S. Kumar, "Dynamic anomaly detection using cross layer security in MANET," Computers & Electrical Engineering, vol. 59, pp. 231–241, 2017.
[33] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET," Wireless Networks, vol. 24, no. 8, pp. 2957–2971, 2018.
[34] M. Thebiga and R. SujiPramila, "A new mathematical and correlation coefficient based approach to recognize and to obstruct the black hole attacks in MANETs using DSR routing," Wireless Personal Communications, vol. 114, no. 2, pp. 975–993, 2020.
[35] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in MANET," in in 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 818–824, IEEE, 2017.
[36] S. Gurung and S. Chauhan, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," Wireless Networks, vol. 25, no. 3, pp. 975–988, 2019.
[37] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in in 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pp. 1–6, IEEE, 2016.
[38] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," in in 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 525–530, IEEE, 2016
[39] S. Shrestha, R. Baidya, B. Giri, and A. Thapa, "Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol," in in 2020 8th International Electrical Engineering Congress (iEECON), pp. 1–4, IEEE, 2020.
[40] S. Hossain, M. S. Hussain, R. R. Ema, S. Dutta, S. Sarkar, and T. Islam, "Detecting black hole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET," in in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7, IEEE, 2019.
[41] D. A. F. B. H. INTRUSION, "Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks," Journal of Computer Science, vol. 9, no. 4, pp. 521–525, 2013.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[42] S. R. Deshmukh, P. Chatur, and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," in in 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)., pp. 1960–1964, IEEE, 2016
[43] V. Savkare and N. Kazi, "AODV and DSR routing protocol performance comparison in MANET using network simulator (NS2)," Int. Res. J. Eng. Technol, vol. 6, no. 9, pp. 7–10, 2019.
[44] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 28–33, IEEE, 2019.
[45] R. Skaggs-Schellenberg, N. Wang, and D. Wright, "Performance evaluation and analysis of proactive and reactive MANET protocols at varied speeds," in in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 981–985, IEEE, 2020.
[46] A. Pramanik, B. Choudhury, T. S. Choudhury, W. Arif, and J. Mehedi, "Behavioral study of random waypoint mobility model-based energy aware MANET," in in 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 624–629, IEEE, 2016.
[47] R. Thiagarajan and M. Moorthi, "Efficient routing protocols for mobile ad hoc network," in in 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), pp. 427–431, IEEE, 2017.
[48] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in MANET," Procedia Computer Science, vol. 151, pp. 1176–1181, 2019.
[49] Z. Ahmad and A. Bansiya, "Survey on security by using intrusion detection system in MANET," A RKDF University Journal of Science and Engineering, vol. 2, no. 1, pp. 21–25, 2019.
[50] S. Sivanesh and V. S. Dhulipala, "Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks," Mobile Networks and Applications, 2020.
[51] V. Nancy, "A security for MANET interruption recognition & preclusion approaches for network layer attacks," International Journal of Applied Engineering Research, vol. 13, no. 12, pp. 10702–10706, 2018.
[52] T. K. Saini and S. C. Sharma, "Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept," Ad Hoc Networks, vol. 103, p. 102148, 2020.
[53] A. Zrelli, H. Khlaifi, and T. Ezzedine, "Performance evaluation of AODV and OAODV for several WSN/IoT applications," in in 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6, IEEE, 2019.
[54] N. Kamboj and M. Rai, "A new secure ad-hoc on demand distance vector routing protocol to ensure less power consumption in mobile ad-hoc network," Journal of Computational and Theoretical Nanoscience, vol. 17, no. 6, pp. 2483–2487, 2020.
[55] T. A. S. Srinivas and S. M. Manivannan, "Preventing collaborative black hole attack in IoT construction using a CBHA–AODV routing protocol," International Journal of Grid and High Performance Computing, vol. 12, no. 2, pp. 25–46, 2020.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)