WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comparison between Black Hole and Flooding Attack inMobile Ad-hoc Network and their Simulation Study

Amal S. Al Maamari [1] **, *Nadir K.Salih*** [2]

Electrical and computer Department, College of Engineering, University of Buraimi, Oman[1,2]

DOI: https://doi.org/10.55248/gengpi.2022.31202

ABSTRACT

Mobile ad hoc network (MANET) is dynamic in nature and vulnerable for several attacks to be arising in it. Mobile nodes frequently disconnect and join the network; they can arbitrarily moves from one place to another. In present-day wireless communication scenario, Mobile ad hoc network (MANET) plays a very important role, as it consists of many autonomous nodes which communicate together to form a proper communication network. Each node in a network will move in random path, so that nodes direction will change frequently. This paper describes the features, application, flooding attack and black hole attack in the MANET implemented on AODV protocol. The simulation work is carried out in Network Simulator (NS2.34). The performance analysis is done Nodes with 20 to 60 nodes were used in the AODV routing protocol simulation to produce energy-efficient outcomes, with the flooding attacks and the interruption of blackhole attacks. The average delay, routing overhead, packet drop rate and packet delivery rate are calculated. By the simulation it has been evaluated that in flooding attack the routing overhead is more as compared to the black hole attack. A comparative study is also done on these parameters for all three scenarios. Also we simulated the attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations.

Key word: Mobile ad hoc network, Black hole, flooding, autonomous nodes

I. Introduction

The MANET is a relatively new technology in places where managing and maintaining massive infrastructures would be prohibitively costly, such as war zones, natural disaster zones, PDAs, and industrial sensors[1][2][3]. Nevertheless, it is possible to use MANET to define its features, such as their mobile communication modes where topologies self-organize are generated on the fly[4]. The infrastructure of the network and mobility has generated interest in new research and development because of its sporadic nature[5][6][7]. In addition, wireless communication is so mobile, and two primary performance and reliability concerns are common with this network security type[8]. It is fundamental for a MANET climate to defeat specific impediments and shortcomings like path-loss, Eavesdropping, blockage, and obstruction, which add to non-line of sight channels where network nature relies upon terrain. It likewise contains a radio band that results in lower data rates than remote organizations along these lines ideal utilization of breaks [9][10]. Figure 1 describes the randomness of the nodes' movements, which often results in partitioning the network's connections. This primarily impacts the nodes in between [10][11]. Compared to BGP, MANETs suffer from greater packet loss due to variables including concealed terminals that create wireless channel problems (high BER), collisions, frequent breaks, and interference in routes caused by node mobility[12][13][14]. As part of this attack, the target black hole node attempts to promote itself as having the quickest route by sending bogus RREPs to route requests [15]. These fake RREPs trick the source into sending network traffic to the black hole node, where it may be snooped on or absorbed to cause the data packets to be dropped[16][17].

Figure 1 Randomness of the nodes' movements

MANETs are distinct networks as compared with infrastructure-based networks. In this network, every node in the network has autonomous behavior, multi-hop routing networking, and decentralized firewall; hence the network architecture is dynamic [17][18][19]. MANET has an absolute symmetric environment with a mobility and high user density. Researchers are drawn to MANET because of its unique qualities, but the technology is beset by drawbacks and obstacles that restrict its overall performance and security. Figure 2 shows an example of MANET in action [20][21].

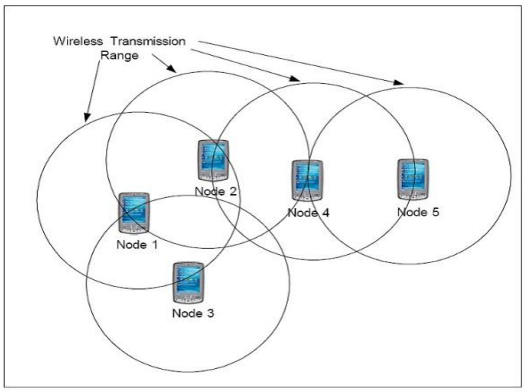

Fig. 2: MANET nodes and transmission ranges.

As Node 2 said, it wants to distribute data. Routes are discovered, and packets are exchanged between the two nodes. The second device, if it is a hostile device, claims to have a path to the target and promptly communicates in response to the action of node S. if the malicious node 2 replies first, then affects node S. Node S assesses that route immediately and starts to connect with node 2 by transmitting data packets. S ignores all earlier responses. Cooperative black hole attacks happen when several bad actors work together to absorb data packets, nodes work together. Hostile node utilizes its routing protocol in a black hole attack. Because of the dissemination of fake news, having a tiny target node's route it promotes no matter how many times you check the table for routing in this black hole node. In the attacker's node, there will always be and therefore intercept the response to the route request the packet of data and keep it. The querying party will receive the black hole node response in a protocol based on floods. Node before it receives a reply from the real node, thus a dark hole when this route is set up, the node can drop all packets or send them on to the unknown destination. An attacker advertises the quickest way to the destination device via the routing protocol in a Black Hole Attack. An attacker retains an eye on the routes requested in a flooding-based system. It is also uncommon for the attacker to react by creating a concise route when asked to route to the destination node [22][23]. A false route is formed if the malicious response reaches the starting node before the legitimate node's reply[24][25].

II. Related Work

Mutu and Saleh in [29] they proposed that black-hole identification has been a hot research topic. Researchers have proposed several approaches for detecting and dealing with black hole attacks. However, only a few of them can spot collaborative black holes. Mujeeb in [22] he described to prevent the blackhole attack, and a proposed technique built a grid in the network. Every grid has a sink node that monitors the behavior of the nodes and locates the untrusted nodes. The network is then cleared of any untrustworthy or blackhole nodes. Singh in [18] he proposed a network with no permanent infrastructure name as MANET made up of mobile nodes arranged dynamically. This network is always self-contained. Power and mobility constraints limit their ability to provide for themselves. Anonymity, security, integrity, availability, and authentication to all mobile communication users are all critical in these networks[26][27]. In MANET, there are a variety of security attacks that cause communication failure from source to destination. One of the more significant assaults in MANET is the black hole attack [28]. This study compared existing solutions and addressed various methods for preventing the black hole attack in MANET[46]. MANETs permit mobile devices to communicate altogether over a network through infrastructure-less or a decentralized authority [30][31]. In MANETs, nodes can enter or exit the network at any time, resulting in dynamic topologies [32][33]. MANETs are in danger of various malicious assaults, necessitating the use of a security design approach. Kim et al., [19] they proposed a flooding detection method using encounter record data to separate flooding attacks from legal burst transmission in delay tolerant networks[47][48]. Nevertheless, using digital signatures and exchanging encounter information among nodes results in a large network overhead and power expenditure [34][35]. The authors Tsiota et al., in [20] they proposed that several techniques have been implemented as a corrective to a flooding assault security worthy based scheme, FAP scheme, and effective filtering approach. Each method has a different strategy for dealing with opponents [36][37]. A policy-based detection technique based on packet knowledge from neighbors has been developed in this regard. This method aids in detecting an attacker's real-time behavior and the isolation of the malicious node from the network [38][39]. Sheikabdullah et al., in[21] they stated that due to a lack of centralized monitoring, MANETS endanger several sorts of assaults. This study examines the effect of a black hole attack on the MANET network layer under different conditions[40][41]. Assuming to be the most cost-effective route to the target, this kind of network layer assault is known as the "BH attack" MANETs employing the routing protocol of AODV with and without a BH attack may be simulated using the NS-2[42][43]. The speed of a node, the number of a node, and as well as the number of BH nodes, and the number of fluxes are all variables that may be changed to produce various outcomes[44][45].

III. Implementation and Results

The results of these assaults are presented in this section and are integrated into the NS. To comprehend the simulation situations, we first went through the Tcl language in this section. Next, we discuss the Blackhole and flooding attacks simulation to highlight its impacts after showing, and then we tested the Blackhole and flooding attacks execution and implementation. This research utilized the UDP protocol to get accurate results from the simulations. Even if the hostile node drops UDP packets, the source node continues to send them, while if the TCP protocol is used, the node completes the connection. As a result, were able to see the flow of information between the sending and receiving nodes throughout the simulation. The Tcl script displayed in Figure 3 was used to add the Black Hole and flooding effect to Node 0 by just striking out three statements. The first line, "$ns node-config -Adhoc Routing blackhole AODV," adds the Black Hole AODV behavior to all nodes built after that.

```
# $ns node-config          -adhocRouting blackholeAODV
set node_(0) [$ns node]
# $ns at 0.0 "$node_(0) label \"BlackHoleAODV Node\""

# $ns node-config          -adhocRouting AODV
set node_(1) [$ns node]
set node_(2) [$ns node]
$ns at 0.0 "$node_(2) label \"Sending Node\""

set node_(3) [$ns node]
set node_(4) [$ns node]
set node_(5) [$ns node]
$ns at 0.0 "$node_(5) label \"Receiving Node\""

set node_(6) [$ns node]
```

Figure 3 Node creation and configuration in Tcl script

Black Hole's AODV version was tested using our test. After that, we have executed the actual simulation, which we will go over in the upcoming session. Unfortunately, because of the high number of connections and nodes in the actual simulation, we could not observe the effects of the BH AODV Node in a short simulation with a small number of nodes. The simulation results are obtained from the output trace file of the Tcl programs. All events in the simulation are recorded in trace files, including when packets are delivered, which node created them, which node received them, which sort of packet is transmitted, why it was lost, and so on. We utilize the “new-trace” file type in our simulations, primarily used in wireless networks and contain extensive event information. We presume that the initial RREP will arrive from the Black Hole since the black hole sends an RREP message without verifying the tables. This concept may or may not work in various circumstances. For example, the second RREP message may arrive at the source node from an intermediate node with up-to-date information on the destination node, or it could arrive from the BH node if the true destination node is closer to the BH node. The number of examples we presented can be expanded based on the network topology's node conditions. Our research investigated how this method reduces BH effects in an AODV network and if it degrades network performance.

A. Results from Terminal

The files used in figure 4 shows the scenario that simulated using UDP and 512 bytes of data, with a simulation time of 100 seconds. Simulated networks include a regular network with no attacks, one with an attack node known as a "black hole," and one that consists of a node-distribution attack known as "node flooding." At this point, the outcomes data will be analyzed and documented in the form of tables and graphs from the simulation environment that has been run. Packet loss, end-to-end latency or delay of transmission, energy, and throughput are among the results of the testing environment of performance while utilizing UDP packets in every scenario. Applications like NS2, Ms. Excel, and NAM are used to test each of these situations.

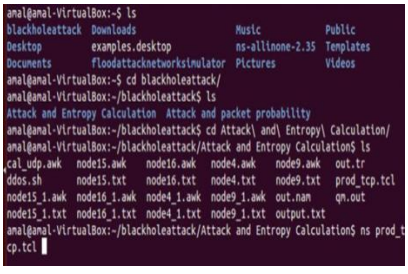

Figure 4 file of Black Hole Attack in Terminal

Native AODV throughput is lower when there is a BH node in the network due to various packet losses incurred by the node. Native AODV had the maximum throughput since there was no flood attack node in the network. A flood attack node can increase the throughput of the TBBT network, but if there is no BH node in the network, the TBBT network has a lower throughput than the original AODV. In addition to having a black hole in the path

between source or sender and destination or receiver nodes, TBBT discards any response from unknown nodes, which reduces throughput. The results of terminal to both black hole and flood attacks depicted in figure 5 and figure 6.

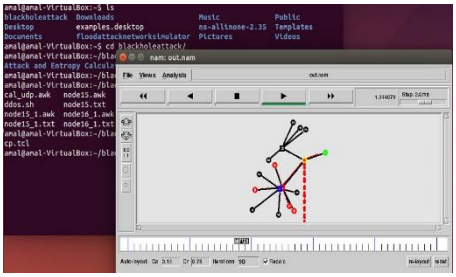

Figure 5 Black Hole Full Terminal Results

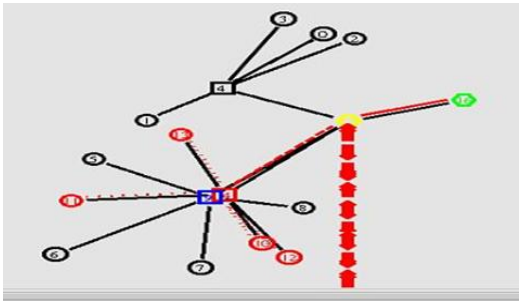

Figure 06 Flood Attack Terminal Results

There were zero Throughput results for native AODV against cooperative flood attack nodes, because the quantity of flood attack nodes grows exponentially, preventing the sender nodes from connecting. Due to it is increase in the number of attack nodes in TBBT AODV as shown in Figure 7.

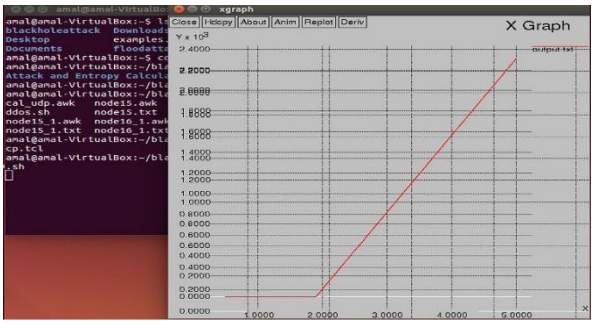

Figure 7 AODV Flood Attack

B. NetAmin Results

NetAnim is a Qt-based offline animator. For now, it uses XML trace files gathered throughout the simulation to generate animations. George F Riley created the initial version. Selecting animation file from Ns directory the packets are moving from one node to another node, as shown in the figure 8. Figure 9 shows the netanim view of the terminal simulations to represented packet delivery ratio for two types of attack. It defines the IP and mac addresses of the moving nodes and stats of the moving nodes. It clearly sees that nodes transfer high throughput when no attack in the network.

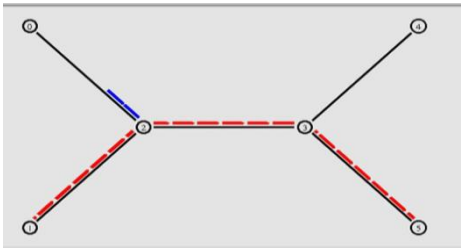

Figure 8 Main Netanim Window

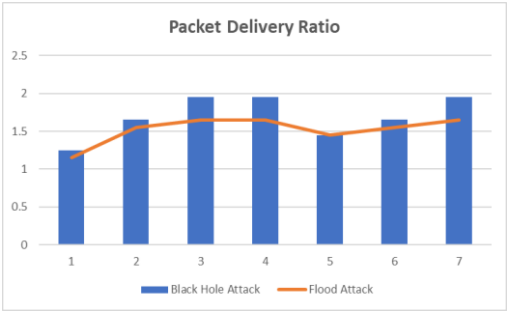

Figure 9Packet Delivery Ratios

C. Comparison Tables

The simulation results are shown in Table 1. In the table for the AODV protocol, we can plainly see the transmitted packets, received packets, and loss percentage. This assumption is taken into account to ensure that the node's position and distance can be determined utilizing the node delimitation procedure. Delay, Packer Delivery Ratio, and Throughput are being used as appraisal measures.

Table 1 Black Hole Attack for AODV

Nodes	Sent Packets	Received Packets	Loss
10	1198	1170	28
20	1190	1158	32
30	1180	1142	38
40	1155	1153	2
50	1025	998	27
60	978	960	18
70	682	675	7

Table 1 and Table 2 illustrate the possibilities for simulating the AODV protocol, even without black hole nodes, using stated parameters. Different node placement and movement arrangements were also investigated for each situation, with the notion that a node's location is fixed once data transmission begins. The node separation method assumes this assumption to ensure that the node's location and distance can be computed. Delay, Packer Delivery Ratio, and Throughput are some of the evaluation measures used.

Table 2: Flood Attack Scenario

Nodes	Sent Packets	Received Packets	Loss
10	1198	1146	52
20	1190	1132	58
30	1180	1140	40
40	1155	1150	5
50	1025	988	37
60	978	952	26
70	682	668	14

D. Graphs Comparison

After receiving an RREP message from another node, the malicious one will produce it as RREP with an abnormally large number in the DSN field and unicast it to the source node. There's no need to worry about other RREP packets when the source receives this one since it assumes the malicious node has the quickest and most current path to the destination and disregards all other RREP packets. In the event of a rogue node receiving data packets, they are not forwarded to other nodes. Figure 10 shows the greatest End-to-End Jitter in native AODV when a black-hole node is in the network. It was found that End-to-End jitter was lowest when no black-hole node was present because the AODV technique used in determining the shortest line was used.

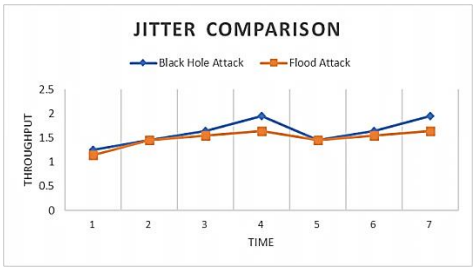

Figure 10 Jitter Comparison

Figure 11 shows the information acquired from comparing the value of packet drop outcomes for scenarios A, B, and C. With a high packet loss value, the network state is deemed unfavorable. For example, scenario B, with the number of nodes 60, has the highest packet loss value of 95.31 percent, whereas scenario A with the number of nodes 20 has the lowest packet loss value of 32.444 percent. As the above shows, the packet delivery ratio of Tapping AODV is superior to the AODV method as the number of black hole nodes grows? It also has a graphical form, which is seen in the graph.

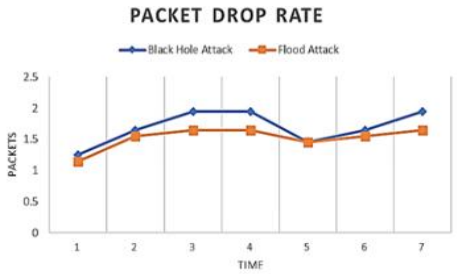

Figure 11 Packet Drop Rate

Figure 12 shows that throughput values in scenarios A, B, and C can be compared using the results. Again, there is a low throughput because of poor network conditions. With 60 nodes, scenario B has the lowest throughput at 48.744 Kbps, whereas scenario A with 20 nodes has the highest at 702,088 Kbps.

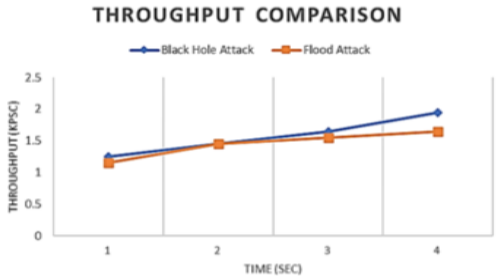

Figure 12 throughput Comparison

Tests were conducted using our test for Blackhole and flooding attacks AODV version. We'll go through the real simulation in the future session, which we conducted after that. Unfortunately, a short simulation of the Black Hole AODV Node was unable to show the impacts of this node due to the enormous number of nodes and connections in the real network simulation.

IV. CONCLUSION

Black hole and flooding nodes are relatively common MANET attack nodes. A complete simulation model with black hole and flooding nodes is presented and corresponding experiments of each attack type in the model are made to validate their different effects to the network performance. Experimental results show that the network performance are various in different attack situations. The model can accurately simulate the impact of black hole and flooding attacks on the key performance indicators of network which can provide reliable test environment for the research of MANET route security and can also provide reference for the research of the information counter technology in Adhoc Network. Currently, in terms of the prohibit methods to black hole and flooding node attacks, the easiest and most common one is to prohibit intermediate node responding RREQ message and only allow the destination node to reply RREQ messages. This method, though to a certain extent, can defense black hole and flooding attacks, but on no doubt that it increases the network burden resulting in the increase of route discovery delay and network routing load and therefore, affect the network performance.

Future research might attempt to find the black hole node using connection-oriented protocols to prevent the black hole and flooding node attacks effectively and minimize the consumption of system resources as much as possible.

REFERENCES

[1] Kumar, D. & Bhartiya, R., 2016. A detailed study on black hole attack in MANET. International Journal of Computer Applications, 146(3), pp. 975–8887.

[2]Elejla, O. E., Belaton, B., Anbar, M. &Smadi, I. M., 2017. A New Set of Features for Detecting Router Advertisement Flooding Attacks. Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017, pp. 1–5.

[3] Kim, B. S., Majengo, D. G., Kim, K. il, Roh, B. S. & Ham, J. H., 2019. Dynamic timer based on expected link duration in Mobile Ad Hoc Networks. Proceedings - 2019 IEEE 16th International Conference on Mobile Ad Hoc and Smart Systems Workshops, MASSW 2019, pp. 158–159.

[4] Kapur, R. K., 2015. Analysis of attacks on routing protocols in MANETs. Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015, pp. 791–798.

[5] Praveen, K. S., Gururaj, H. L. & Ramesh, B., 2016. Comparative analysis of black hole attack in Ad Hoc Network Using AODV and OLSR Protocols. Procedia Computer Science, 85, pp. 325–330.

[6] Tsiota, A., Xenakis, D., Passas, N. &Merakos, L., 2019. On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks. IEEE Transactions on Vehicular Technology, 68(11), pp. 10761–10774.

[7] Abu Zant-Yasin 2019 Mahmoud Abu Zant, Adwan Yasin, "Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)", Security and Communication Networks, vol. 2019, Article ID 8249108, 12 pages, 2019. https://doi.org/10.1155/2019/8249108.

[8] Rani, P., Kavita, Verma, S. & Nguyen, G. N., 2020. Mitigation of black hole and gray hole attack using swarm inspired Algorithm with Artificial Neural Network. IEEE Access, 8, pp. 121755–121764.

[9] Omprakash, S. H., 2020. Mitigation technique for black hole attack in Mobile Ad hoc Network. 2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020.

[10] Mujeeb, A., 2020. Modeling and Detection of Flooding-Based Denial-of-Service Attack in Wireless AdcuiHoc Network Using Bayesian Inference. IEEE Systems Journal, 15(1), pp. 1–10.

[11] Fiade, A., 2020. Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network). 2020 8th International Conference on Cyber and IT Service Management, CITSM 2020, pp. 6–10.

[12] Mutu, L., Saleh, R. &Matrawy, A., 2015. Improved SDN responsiveness to UDP flood attacks. pp. 715–716.

[13] Singh, A. K., Shukla, Y., Kumar, N. & Rout, M., 2019. Impact of ART and DPC on AODV Routing Environment for Dynamic Network using QualNet 7.1. Proceedings - 2019 International Conference on Electrical, Electronics and Computer Engineering, pp. 1–6.

[14] Oakley, I., 2020. Solutions to Black Hole Attacks in MANETs. 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP 2020. pp. 21-26.

[15] Elmahdi, E., Yoo, S. M. &Sharshembiev, K., 2018. Securing data forwarding against blackhole attacks in mobile ad hoc networks. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC 2018, 2018-January, pp. 463–467.

[16] Sheik Abdullah, R. &Hariganesh, S., 2017. OTPR-Optimum Transmission Power Routing against Black Hole Attacks in MANETs. Proceedings - 2nd World Congress on Computing and Communication Technologies, pp. 0–3.

[17] Ghaffari, A., 2020. Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks. J Ambient Intell Human Comput 11, 1593–1603. https://doi.org/10.1007/s12652-019-01316-z

[18] Liu, Chen,Yu .,2018. An Intersection-Based Geographic Routing with Transmission Quality Guaranteed in Urban VANETs DOI 10.1109/ICC.2018.8422935

[19] Qureshi, K.N., Bashir, F. & Abdullah, A.H., 2020. Distance and signal quality aware next hop selection routing protocol for vehicular ad hoc networks. Neural Comput&Applic 32, 2351–2364. https://doi.org/10.1007/s00521-019-04320-8

[20] Singh, K., 2015. Performance analysis of security attacks and improvements of routing protocols in MANET. 2015 2nd International Conference on Computer Science, Computer Engineering, and Social Media, pp. 163–169.

[21] Vimal, V., 2017. Plummeting flood based distributed-DoS attack to upsurge networks performance in ad-hoc networks using neighborhood table technique. IEEE Region 10 Annual International Conference, pp. 139–144.

[22] Wei, H., Tung, Y., Yu, C., & Security, A. N. (2016). Counteracting UDP Flooding Attacks in SDN. 367–371.

[23] Shankar, K., &Elhoseny., 2019. Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES. J Univers. Comput. Sci., 25, 1221-1239.

[24] Rajendra Prasad P, Shivashankar., 2021. ENHANCED ENERGY EFFICIENT SECURE ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORK, Global Transitions Proceedings, 2021,

[25] Kaysina, I. A., Vasiliev, D. S., Abilov, A., Meitis, D. S., &Kaysin, A. E., 2018. Performance evaluation testbed for emerging relaying and coding algorithms in Flying Ad Hoc Networks. Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - Proceedings, 2018-March, pp. 1–5.

[26] Sivanesh, S. & Dhulipala, V. S., 2019. Comparitive Analysis of Blackhole and Rushing Attack in MANET. In 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), pp. 495-499.

[27] Srivastava, S. K. & Raut, R. D., 2019. Enilariems the performance of average throughput, end-to-end delay, drop packets and packet delivery ratio by using improved AODY (AODY+) routing protocol in ad-hoc wireless networks. Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, pp. 266–269.

[28] Karuppiah, A. B., Dalfiah, J., Yuvashri, K., & Rajaram, S., 2015. An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks. In International confernce on innovation information in computing technologies, pp. 1-7.

[29] Singh, B., 2016. Mitigating effects of Black hole Attack in Mobile Ad-Hoc Networks: Military perspective. Pp. 810–814.

[30] Jain, A. &Shrotriya, A., 2016. Investigating the effects of black hole attack in MANET under shadowing model with different traffic conditions. IEEE International Conference on Computer Communication and Control, IC4 2015.

[31] Mahore, H., Agrawal, R., & Gupta, R., 2018. Agent based black hole detection technique in AODV routing protocol. 2018 International Conference on Advanced Computation and Telecommunication, (ICACAT), pp. 1-6.

[32] Raj, P. N. &Swadas, P. B., 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet.

[33] buZant-Yasin 2019 Mahmoud Abu Zant, Adwan Yasin, "Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)", Security and Communication Networks, vol. 2019, Article ID 8249108, 12 pages, 2019. https://doi.org/10.1155/2019/8249108

[34] Ali, S., Khan, M. A., Ahmad, J., Malik, A. W., & Ur Rehman, A., 2018. Detection and prevention of black hole attacks in IOT & WSN. pp. 217–226.

[35] Arya, N., 2015. Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. 2015 International Conference on Computer, Communication and Control (IC4).

[36] Biagioni, E., n.d. Preventing UDP flooding amplification attacks with weak authentication. 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 78-82.

[37] Chadha, K. & Jain, S., 2014. Impact of black hole and gray hole attack in AODV protocol.

[38] Cui, B. & Yang, Y., 2018. Hotspot-based Resource Sharing System for Mobile Ad hoc Networks. Proceedings of 2018 IEEE 8th International Conference on Electronics Information and Emergency Communication, ICEIEC 2018, pp. 146–149.

[39] Nadir K Salih, Tianyi Zang. Variable service process by feature meta-model for SaaS Application. IEEE International Conference in Green and Ubiquitous Technology, IEEE, 2012, pp102 – 105. EI (20125015791678).

[40] Nadir K Salih, Tianyi Zang. Autonomic and cloud computing: Management Services for Healthcare. IEEE International Symposium on Industrial Electronics and Applications (ISIEA 2012) EI (20131816295185).

[41] Nadir K Salih, Tianyi Zang. Modeling and Self-Configuring SaaS Application. International conference on software engineering research and practice (SERP14), held in July 21-24 Las Vegas,USA.- 2014. (SCI).

[42] Nadir K Salih, Tianyi Zang. Autonomic Management for Applicability and Peformence in SaaS Model. International conference on parallel and distributed processing techniques and applications (PDPTA'14), held in July 21-24 Las Vegas,USA.- 2014.(SCI).

[43] Nadir K Salih, Tianyi Zang. Self-management SaaS Application by CBR Algorithm . International conference on parallel and distributed processing techniques and applications (PDPTA'17), held in July 21-24 Las Vegas,USA.- 2017.

[44] Nadir K Salih, Tianyi Zang. Implementation of Autonomic Management SaaS System . conference on software engineering research and practice (SERP14), held in July 21-24 Las Vegas,USA.- 2017.

[45] GK Viju, Nadir K Salih, Tianyi Zang. A novel approach to iris recognition for personal authentication. International Conference of Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE., IEEE, 2011, pp 350-354. EI (20121314902019).

[46] G.K.Viju, Nadir K.Salih. A secure multicast protocol for ownership rights. International Conference of Computing and Information Technology (ICCIT), 2012, pp 788-793.

[47] Sheima S. El-hwaij, Nadir K.Salih. Autonomic management by self-optimization for WEINMANN. IEEE, International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), 2017.

[48] Nadir K.Salih, D Satyanarayana , Abdullah Said Alkalbani, R. Gopal. A Survey on Software/Hardware Fault Injection Tools and Techniques. IEEE Symposium on Industrial Electronics& Applications (ISIEA2022).