PERFORMANCE ANALYSIS OF AODV AND DSR ROUTING PROTOCOLS UNDER BLACKHOLE ATTACK USING NS-2

Ferdinand Alifo[1], Mustapha Awinsongya Yakubu[2],
Martin Doe[3] and Michael Asante[4]

[1]MIS/Computer Dep., Ministry of Local Government,
Local Gov't Service, Ghana
[2]University of Cincinnati Ohio, USA
[3]Computr Science Department, University of Business and Integrated
Development Studies, Ghana
[4]Department of Computer Science, Kwame Nkrumah University
of Science and Technology, Ghana

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are wireless networks without a fixed infrastructure, allowing nodes to move freely and act as both routers and hosts. Nodes establish virtual links and use routing protocols like AODV, DSR, and DSDV for connections. Security is a concern, with the Blackhole attack being a notable threat where a malicious node drops packets instead of forwarding them. The paper used NS-2.35 ns-allinone-2.35 version for simulating the impact of Blackhole nodes and implementing AODV and DSR protocols. The study analyzed average throughput, packet delivery ratio, and residual energy as metrics, observing that AODV showed better energy efficiency and delivery than DSR, but DSR performed better in throughput. Environmental factors and data sizes were also considered in the analysis.

KEYWORDS

Performance Analysis, AODV, DSR, MANET, Protocols, Security, Blackhole, Metrics, Attack, NS2

1. INTRODUCTION

Routing protocols play a significant role in MANET research, with a focus on ensuring effective and secure communication. Numerous routing protocols have been developed expressly for MANETs, such as AODV, DSR, DSDV, OLSR, and others. MANETs face vulnerabilities due to factors like an open access medium, dynamic topology changes, lack of central administration or monitoring systems, cooperative algorithms, and transparent protective mechanisms (Jatin Jindal et al., 2015). The appealing qualities of MANETs make them susceptible to malicious activities. It is essential to prioritize security concerns in order to improve network availability, data reliability, and privacy. Since MANETs operate wirelessly, they are vulnerable to various forms of attacks including Blackhole attacks, saturating attacks, routing table overflow attack, Denial of Service (DoS) attack, Sybil attack, impersonation attacks, and others (Patra et al., 2020). These threats jeopardize the availability, integrity, and confidentiality of network services.

David C. Wyld et al. (Eds): ICDIPV, CBIoT, ICAIT, WIMO, NC, CRYPIS, ITCSE, NLCA, CAIML -2023
pp. 485-496, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131339

The Blackhole Attack is one of the most dangerous attacks on MANETs and represents a significant risks. The Blackhole Attack has been observed to impact MANET reactive routing protocols like Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) (Vanaja and Pinto, 2019). It is therefore essential to address network security issues to enhance network services' availability, and protect user privacy.

1.1. Objective

The primary objective of this paper is to use the NS2 Simulator to examine the performance of the AODV and DSR protocols using several metrics, including Average Throughput, Packet Delivery Ratio (PDR), and Residual Energy at the destination node in Mobile Ad Hoc Networks (MANET).

1.2. Aim

The aim of this work is to evaluate the response of the AODV and DSR routing protocols to a Blackhole attack. To look at how this security risk affects variables like packet delivery ratio, average throughput, and residual energy. Additionally, it seeks to add to the body of knowledge on examining routing protocol performance in the context of security attacks by gaining insights into the behaviour and efficacy of AODV and DSR during the black hole attack.

1.3. Justification of the Study

MANETs gain popularity for wireless network connectivity across sectors due to ease of deployment and freedom from cables. However, they are vulnerable to security attacks like Blackhole attacks. Analysing AODV and DSR routing protocols under Blackhole attacks provides valuable insights into these vulnerabilities.

1.4. Structure of the Paper

The study primarily investigates two MANET protocols, namely AODV and DSR, and their shared characteristics. It delves into literature which necessitates specialized knowledge to comprehend the subject matter. Methodology outlines the installation procedures and conducts simulation experiments. The results and analysis evaluates the performance of AODV and DSR, considering relevant metrics frameworks. In Conclusion, the study provides a summary of its findings, and offers recommendations for future research.

1.5. Related Work

A number of researchers have compared these MANET Protocols to selected security attacks, as recorded in Table 1, which highlights earlier research on MANET.

Table 1. A comparison table showing existing research work.

Author(s)	Attack Type Addressed	Routing Protocol	Routing Metrics	Simulation Tool
Obiniyi et al. 2015		Proactive and Reactive		
Sairam et al, 2019	Blackhole	AODV	End-to-end delay, umber of packets dropped and Throughput	NS2
Arage & Satyanarayana 2018	Blackhole, warmhole, etd	DSR	Throughput, Delay, PDR	NS2
Khalid et al. 2020		Proactive and Reactive	Throughput, Delay, PD and Fraction	
Panda and Pattanayak 2018	Blackhole	AODV, DSR	End-to-end Delay, PDR, Throughput	NS2.35
Patra, et al, 2020	grayhole, warmhole etc	Proactive and Reactive	Throughput, end to end and PDR	NS2
Awadhesh et al, 2013		AODV, CBRP, DSDV and	Minimum and maximum delay, Packet Delivery Ratio,	NS2
		DSR	Throughput	
Iqbal et al, 2018		AODV	PDR, Energy lifetime, E2E, Throughput	NS2

2. LITERATURE REVIEW

In this chapter, we conducted an in-depth examination of the two reactive (on-demand) routing protocols, with the focus on the AODV protocol and the DSR protocol.

MANET, or infrastructure-less network, is adaptable and self-organizing, enabling continuous device connections without fixed infrastructure (Obiniyi et al., 2015). However, in decentralized environments with dynamic topologies, routing messages becomes challenging. There is a wireless interface on each node to make communication easier.

2.1. Routing Protocols Under Manets

Reactive, proactive, and hybrid routing protocols constitute the three main protocols used in MANETs.

Proactive Routing protocols use a vector or DSDV routing mechanism, which was built using the Bellmann-Ford approach and the order of arrival. All information about the available nodes is kept in the routing table. All mobile nodes must broadcast their entries to other nodes in their adjacency. With mutual consent, the nodes along the path send the data packet from one to the next (Obiniyi et al. 2015).

According to (Panda and Pattanayak 2018) reactive protocols are well recognized as on demand protocols. They are referred to as "on-demand" protocols because they never start the route discovery process on their own; instead, they wait until they are requested to do so,

As stated by (Sairam et al., 2019), the hybrid protocol combines elements from both reactive and proactive routing protocols. In a single solution, it provides the benefits of proactive and reactive routing. These protocols are adaptive, providing information about the zone as well as the starting and stopping places of mobile nodes.

2.2. Review of AODV and DSR

AODV and DSR are most popular reactive routing protocols categorized as flat routing. Unlike proactive protocols, they do not require regular broadcasting (updates) of the routing table, resulting in enhanced network bandwidth utilization. These protocols involve two primary phases: route discovery and route maintenance (Obiniyi et al., 2015)

2.2.1. Ad-Hoc On-Demand Distance Vector (AODV)

According to (Panda and Pattanayak 2018), AODV is a reactive routing protocol that possesses no route information or broadcast it packets. When a source want to establish communication with another node, AODV uses flooding control messages to figure out how to get there. When a sender node wants to send a packet, it looks up the subsequent intermediate hop in its routing database before transmitting the packet. This process is repeated for all consecutive hops.

2.2.1.1. Routing Mechanism in AODV

An important part of AODV is that it keeps track of time-based states. This means that a routing entry that hasn't been used in a while is considered to be out of date. If the route breaks down, the neighbours are told. Using query and reply sequences, the route is determined from the sender to the receiver, and intermediate nodes along the route record route information in the form of route table entries. Control packets are used to find and break routes (Panda and Pattanayak 2018) AODV uses several types of control messages for its route operation mechanism. These include the Route Reply (RREP) message, Route Error (RERR) message, and Hello messagebreaks down, the neighbours are told. Using query and reply sequences, the route is determined from the sender to the receiver, and intermediate nodes along the route record route information in the form of route table entries. Control packets are used to find and break routes (Panda and Pattanayak 2018)

AODV uses several types of control messages for its route operation mechanism. These consist of the Hello message, Route Reply (RREP), and Route Error (RERR) messages.

2.2.1.2. Route Discovery in AODV

When a source node doesn't know how to get to an endpoint, it initiates the route discovery procedure for the node it wants to connect with. RREQ is broadcast to start the method. When the RREP message gets to the destination node, the route is said to be taken. When numerous RREP messages with various routes are received, the RREP message with the highest sequence number is used to update the routing information, and acknowledgement takes place (Obiniyi et al. 2015).

In AODV routing protocol, the route discovery process involves the setup of reverse path and forward path. By setting up the reverse path during the RREQ propagation and the forward path during the RREP propagation, AODV ensures that bidirectional routes are established between the source and destination nodes, allowing for efficient and reliable data transmission in the adhoc network.

2.2.1.3. Advantages of AODV

A significant advantage of the AODV protocol is its ability to discover routes as they are required and utilize destination sequence numbers to identify the current path, resulting in reduced communication setup time.

AODV reacts faster to network topological changes and updates the nodes that are affected by the changes individually.

2.2.1.4. Disadvantages of AODV

With AODV, when a link fails, a massive amount of control messages is generated, which may not inform other routes because frequent updates are not generated.
The AODV routing table takes a long time to develop as the network grows in size, various performance indicators start to deteriorate.

2.2.2. Dynamic Source Routing (DSR)

According to (Arage and Satyanarayana 2018), the DSR routing protocol is one of the most widely used routing protocols in network communication. DSR lets the system organize and change itself without the need for a pre-existing network design or management system. Route Discovery and Route Maintenance are two protocols that operate together to let nodes in MANET networks find and keep track of source routes to any destination

In the DSR, a fatal transmission starts the route maintenance phase, and each node produces route error packets. All routes containing the incorrect hop are truncated at that point when the incorrect hop is deleted from the node's route cache (Obiniyi et al. 2015)

2.2.2.1. Route Recovery in DSR

The DSR protocol was made for multi-hop MANET networks with mobile nodes. DSR permits the network to self-organize and change without the need for a prior network architecture or management system. It does this through Route Discovery and Route Maintenance, two parts of the protocol that work together to let MANETs nodes to find and keep source routes to any destination.

Route Discovery checks the routing cache before data transmission, broadcasting a RREQ if no route information is available or expired. Route Maintenance initiates a RERR if a node fails to find a next hop, re-conducting the route discovery process if it occurs again in DSR (Panda and Pattanayak 2018).

2.2.2.2. Multicast Routing with DSR

DSR makes it possible to send data packets to every node in the MANET-controlled network. The nodes employ destination address filtering to ensure that the packet delivered to the relevant multicast destination address.

DSR adds the data from a DSR packet to a route request that is sent to the multicast address. The standard ROUTE REQUEST propagation mechanism will send this packet to all network nodes quickly and within the number of hops chosen by the sender, which is called the "Time To Live" (TTL). (El-Sayed et al., 2021).

2.2.2.3. Advantages of DSR

DSR employs a reactive approach to periodically notify the network that the table has been updated; as a result, paths to other network nodes are not required. The nodes in between also make good use of the information in the route cache to reduce control overhead and improve network scalability (Arage and Satyanarayana, 2018).

2.2.2.4. Disadvantages of DSR

Because DSR uses a source-routing mechanism, there is also a large routing overhead that may cause network clogging.

Finding the route to the destination may take time and result in network latency. Another problem with DSR is the way it manages broken routes which it does not fix a broken link locally.

2.2.3. Blackhole Attack in MANET

According to (Panda and Pattanayak 2018), a Blackhole attack is an attack where the malicious node advertises itself as having the optimal route to the destination and drops all the packets instead of forwarding them further to the destination. Also, (Sairam et al, 2019) studied that a black hole attack is one kind of routing and distributing attack that can do great damage to the network.

A Blackhole attack exploits route discovery vulnerabilities in on-demand protocols, injecting a false route to the destination. Intermediate attacker nodes send a higher destination sequence number RREP, creating a black hole when misusing traffic. This attack can be severe when the attacker becomes part of multiple routes (Panda and Pattanayak 2018).

2.2.3.1. Types of Blackhole Attacks

There are two types of Blackhole attacks: Single Blackhole attacks, in which a node within the network takes on the role of a Blackhole. Its objective is to intentionally drop or discard all incoming traffic, effectively making the affected routes unusable, and Cooperative Blackhole Attack which involves multiple malicious nodes working together to create a Blackhole. These nodes collaborate to drop or manipulate network traffic, causing disruption and compromising the overall integrity of the network (Panda, and Pattanayak 2018).

2.2.4. Blackhole Attacks in AODV and DSR

Blackhole attacks can be categorized into internal and external types. Internal Blackhole Attacks involve an internal acknowledged node leading the attack, making them difficult to detect and defend against. External Blackhole Attacks block network access, impede operations, and create congestion, neutralizing interior Blackhole attacks (Panda, and Pattanayak 2018).

3. METHODOLOGY

In this paper, we employ the ns-2.35 simulator on Ubuntu LINUX to simulate Blackhole attack on the AODV and DSR routing protocols using Object Tool Command Language (OTCL). This simulation enables us to examine and compare the performance metrics of both protocols when the network was exposed to a Blackhole attack. Through these simulations, we were able to assess the behaviour and effectiveness of AODV and DSR in the presence of such an attack. By

utilizing ns-2.35 as our simulation tool, we were able to evaluate how the Blackhole attack affects the routing protocols and draw significant findings about their performance under the metrics

3.1. Simulation Parameters

Simulation parameters govern a model's actions and qualities, influencing outcomes and findings.

They can be modified to examine various situations or circumstances as shown in table 2.

Table 2. Simulation Parameters

Parameter	**Settings**
Channel type	Channel/Wireless channel
Propagation Model	Propagation/TwoRayGround
Physical Type	Phy/WirelessPhysical
Mac Protocol Type	Mac/802_11
Interface queue type	Queue/DropTail/CMU/PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Maximum packet in queue	50
Number of mobile nodes	17
Routing protocol	AODV and DSR
Transmission Range	550 Meters
Interference Range	550 Meters
Start Time/Stop Time	1 Second/15 Seconds
Packet in queue	5, 10, 15, 20, 25, 30
Number of Blackholes nodes	2

3.2. Routing Topology

Routing topology is the plan arrangement of conceptual elements (nodes) in a communication network. For this study, fifteen (15) legitimate nodes and two (2) malicious nodes were set in the topography of 956m by 600m simulation environment. Two commands nam AODV.nam and nam DSR.nam were executed to invoke network animator (NAM) to show the path for AODV and DSR respectively with N

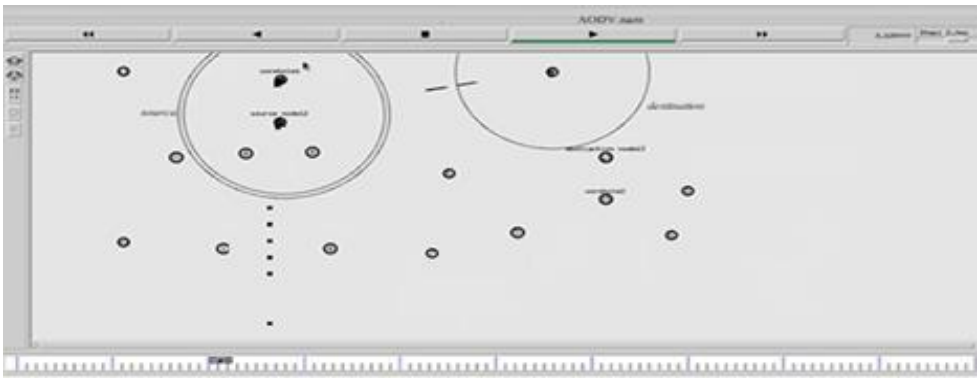

Figure 1: Screenshot of NAM with 17 nodes including two false nodes

3.3. Simulator Execution and setup

Following the successful assembly of NS-2 version ns-allinone-2.35 via Ubuntu on VMware station 16, Six (6) important files required for simulation were copied to the installation folder's home directory for execution.

The Six (6) files comprises of;

- Blackhole.tcl
- average_throu.awk
- energy.awk
- pdr.awk
- AODV.tr
- DSR.tr

Location path for these files; /home/ferdinand/ns-allinone-2.35/ns-2.35/bin:/home/ferdinand/ns-allinone-2.35/Blackhole

#PATH
PATH=$PATH:/home/ferdinand/ns-allinone-2.35/bin:/home/ferdinand/ns-allinone-2.35/tcl11.5.0/unix:/home/ferdinand/ns-allinone-2.35/tk11.5.0/unix

LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/ferdinand/ns-allinone-2.35/otcl-1.14:/home/ferdinand/ns-allinone-2.35/lib
NS=/home/ferdinand/ns-allinone-2.35 /ns-2.35/
NAM=/home/ferdinand/ns-allinone-2.35 /nam-1.14/
PATH=$PATH:$XGRAPH:NS:$$NAM

3.3.1. Simulation Experiment for AODV

After validating the NS-2.35 installation and modifying all of the parameters, changes were made to the Blackhole.tcl file to simulate the AODV routing protocol;

- Interface queue type was set to Queue/DropTail/PriQueue
- Routing protocol was set to AODV tcl file was created as Blackhole.tcl
- trace file was set to tracefile [open AODVblack.tr B]
- nam file for path was set to namfile [open AODVblack.nam B]
- node 10 and node 11 were set as Blackhole node
- packets in queue [5, 10, 15, 20, 25, and 30]

3.3.2. Simulation Experiment for DSR

After validating the NS-2.35 installation and modifying all of the parameters, the Blackhole.tcl file was modified to simulate the DSR routing protocol:

- Interface queue type was set to CMUPriQueue
- Routing protocol was set to DSR
- tcl file was created as Blackhole.tcl
- trace file was set to tracefile [open DSRblack.tr B]
- nam file for topology was set to namfile [open DSRblack.nam B]
- nam file for path was set to namfile [open AODVblack.nam B]
- node 10 and node 11 were set as Blackhole node

4. RESULT AND ANALYSIS

Table 3 showing Average Throughput, Packet Delivery Ratio, and Residual Energy as performance metrics and data sizes displays the simulation results for AODV and DSR.

Table 3: Results of performance metrics for AODV and DSR with data sizes

Protocol	Speed/Data Size	Average Throughput	Packet Delivery Ratio (PDR)	Residual Energy (J)
AODV	5	0.288707	0.993377	1.57784
DSR		0.327946	0.983577	1.410075
AODV	10	0.328707	0.993449	3.155679
DSR		0.367946	0.983725	2.820152
AODV	15	0.368707	0.993521	4.733519
DSR		0.407946	0.983871	4.230228
AODV	20	0.408707	0.99359	6.311358
DSR		0.447946	0.984014	5.640304
AODV	25	0.448707	0.993658	7.889198
DSR		0.487946	0.984155	7.05038
AODV	30	0.488707	0.993724	9.467037
DSR		0.527946	0.984293	8.460455

4.1. Average Throughput Analysis

Average throughput analysis is a technique employed to assess the mean rate at which data is transmitted within a specific time frame in a given system.

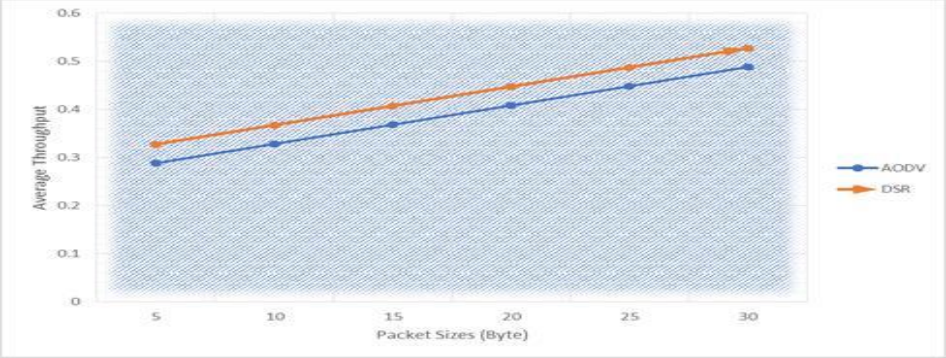

Figure 2. A graph of Average Throughput for AODV and DSR

DSR has higher throughput compared to AODV under Blackhole attack as shown in figure 2, due to its ability to detect and avoid malicious routes, enabling successful packet transmission. Additionally, DSR uses efficient routing mechanisms, reducing overhead and maintaining higher throughput even under attack.

4.2. Packet Delivery Ratio Analysis

Packet Delivery Ratio (PDR) analysis was employed to assess the efficiency and dependability of transmitting data packets within the communication system.

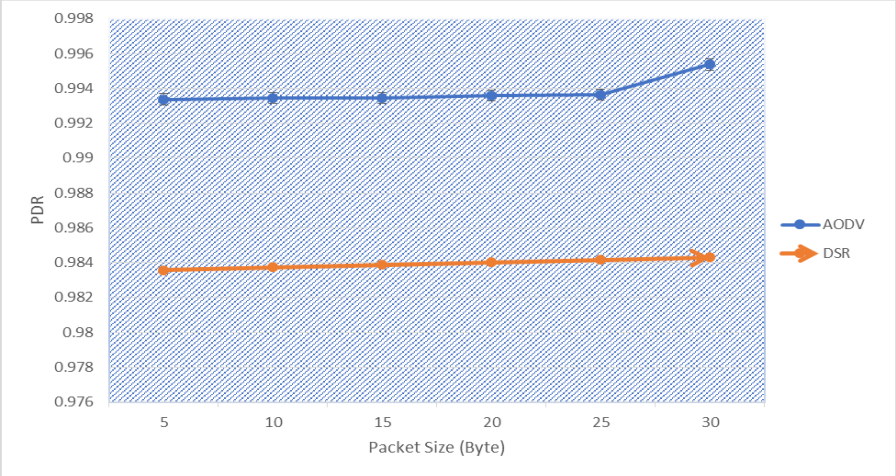

Figure 3. A graph of Packet Delivery Ratio for AODV and DSR

AODV outperforms DSR in PDR under Blackhole attack as shown in figure 3 due to better route detection and avoiding malicious node routes. AODV's efficient routing mechanisms enable lower overhead transmission, ensuring higher PDR even under attack.

4.3. Residual Energy Analysis

Residual energy analysis was utilized to evaluate the energy levels that remain in nodes within energy-constrained systems like wireless sensor networks.

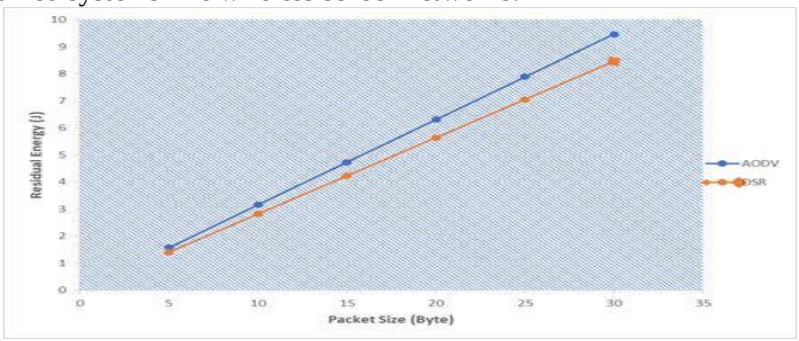

Figure 4. A graph of Residual Energy for AODV and DSR

AODV is more energy-efficient than DSR under Blackhole attack as shown in figure 4, due to its ability to detect and avoid malicious routes, while DSR is more vulnerable. AODV's efficient routing mechanisms require less energy to transmit packets, allowing nodes to conserve energy even during attacks (Zareei et al, 2012).

5. CONCLUSIONS

This study conducted a performance analysis of the AODV and DSR routing protocols under Blackhole attacks, using PDR, Residual Energy, and Average Throughput as metrics. The simulation results indicated that DSR had a higher Throughput but AODV had better PDR and Residual Energy. These findings can help MANET network designers and managers select the best protocols for their unique network requirements

Future work for this study would focus on investigating other performance metrics, evaluating multiple routing protocols, assessing the impact of different attack scenarios, developing and enhancing security mechanisms to mitigate attacks on MANETs, conducting real-world experiments, and deploying the protocols to improve MANET routing protocols.

ACKNOWLEDGEMENTS

We express our gratitude to the reviewers for their thorough examination of the paper, as well as their valuable comments and suggestions that significantly enhanced the quality of the manuscript. Also, our gratitude goes to University of Science and Technology KNUST, Kumasi and University of Cincinnati, Ohio for their support.

REFERENCES

[1] Jatin Jindal, Parminder Singh, & Sukhvir Singh. (2015, June 4). Performance characteristics of DSR, AODV and AOMDV Routing Protocols for MANETs using ns-2: A simulation Study. International Journal of Engineering Research And, V4(06). https://doi.org/10.17577/ijertv4is060100

[2] Panda, Niranjan & Patra, Bichitrananda & Hota, Saebeswara. (2020). MANET ROUTING ATTACKS AND THEIR COUNTERMEASURES: A SURVEY. Journal of Critical Reviews. 7. 2777-2792. 10.31838/jcr.07.13.428.

[3] Vanaja, A & Pinto, Jeevan. (2019). Performance Evaluation of Reactive Routing Protocols in MANETs in Association with TCP Newreno. Journal of Computer Science Research. 1. 10.30564/jcsr.v1i3.1441.

[4] Kaur, N., & Sharma, P. (2016, November 17). The Study and Comparison between AODV, OLSR and DSR Routing Protocols and Attacks in Mobile Ad-Hoc Network. International Journal of Computer Applications, 154(2), 28–31. https://doi.org/10.5120/ijca2016912039

[5] Obiniyi, Afolayan & Oyenike, Mary & Olanrewaju, Oyenike. (2015). Review of Mobile Ad Hoc Network Protocols. IOSR Journal of Computer Engineering (IOSR-JCE) 2278-0661. 17. 2278-661. 10.9790/0661-17220112.

[6] Vamsi, T Sairam & Emani, Raghavendra & Sruthi, T. (2019). Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack. Volume 9. 58-63. 10.9790/9622-0905025863.

[7] El-Sayed, Hamdy H. & Younes, A. & Alghamdi, Fahad. (2021). Multiobjective Multicast DSR Algorithm for Routing in Mobile Networks with Cost, Delay, and Hop Count. Complexity. 2021. 1-8. 10.1155/2021/9965872

[8] Arage Chetan S and Satyanarayana K V V. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 3 (2018) pp. 1605-1612 © Research India Publications. http://www.ripublication.com

[9] Y. Ariyanto, Y. W. Syaifudin, and B. Harijanto. 2017. Performance Analysis of Network Emulator based on the Use of Resources in Virtual Laboratory. In 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2017). Yogyakarta, Indonesia.

[10] Mahdi Zareei, Mohammad Javad Jannati, and Masoumeh Karimi, eConference on Computer and Knowledge Engineering (ICCKE 2012), [online] https://ieeexplore.ieee.org/document/6399004

AUTHORS

Ferdinand Alifo is the Head of ICT/MIS department with Ministry of Local Government in Ghana. He holds an MSc Information Technology from KNUST, a BSc in Computer Science, and His expertise is further validated by his certifications in Cisco Certified Network Professional (CCNP) and Cisco Certified Network Associate (CCNA). mThroughout his career, Ferdinand has made significant contributions to improving IT systems and services within the government and private sectors.

Mustapha Awinsongya Yakubu is a Graduate Teaching Assistant at the University of Cincinnati where he is currently studying for PhD Information Technology. His research focuses in areas of Enterprise Architecture & Security, Human Computer Interaction, and Crisis Informatics. He earned his Master's degree in Information Technology from the Kwame Nkrumah University of Science and Technology. He has over a decade experience working in both public and private sector as an IT Professional.

Martin Doe is the head of the ICT department at Adventist SHTS, Kofiase. He had MPhil in Information Technology at the Department of Computer Science in the Kwame Nkrumah University of Science and Technology, Ghana.He is currently a Ph.D student at the University of Business and integrated development Studies, Ghana. His research area includes Cyber Security and computer networks and internet of things.

Professor. Michael Asante is a Professor at Kwame Nkrumah University of Science and Technology, Computer Science Department, Ghana. A reviewer of journals.