Performance Comparison of AODV and AOMDV Protocol Routing with TCP and UDP on Mobile Ad-Hoc Network (Manet) Using Malicious Node (Blackhole Attack)

Nurul Faizah Rozy[1], Siti Ummi Masruroh[2], Ivan Gustra Manca Armenia[3]
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta-Indonesia
[1)]nurul.faizah@uinjkt.ac.id, [2)]ummi.masruroh@uinjkt.ac.id, [3)]ivangustra@gmail.com

Accepted: 13 Oktober 2019. Approved: 20 Oktober 2019. Published: Nopember 2019

Abstract - **Transmission package delivery can be a problem of routes on the network, one of them is the Wireless network. Mobile Ad-Hoc Network (MANET) topology is often used on Wireless networks. The existence of a malicious node is a threat to MANET. Package delivery uses AODV and AOMDV Protocol Routing in TCP and UDP packet transmission. This study uses a simulation method using NS2, NAM and AWK. The Quality of Service (QoS) parameters used are throughput, packet loss, and jitter. Simulations are carried out using malicious nodes, the results on the AOMDV TCP graph have the highest input values and the best packets but are difficult to minimize energy, while for the TCP jitter values graph is best because it has a flow control function that can adjust the trajectory. The results in AOMDV TCP have the highest input value and the best packet loss but it is difficult to minimize energy, while for TCP value jitters it is best because it has a flow control function that can adjust the trajectory.**

***Keywords:** tcp; udp; manet; aodv; aomdv; malicious node; blackhole attack; ns2; nam; awk; qos; throughput; packet loss; jitter*

I. INTRODUCTION

The growth of technology in Wireless networks is very fast, because it provides high convenience and flexibility for users to be able to establish communication links with others. In wireless networks there are two transmission packages in packet delivery that are used to increase network levels in general, namely TCP and UDP. TCP is a protocol that 75% is mostly used for internet services today. However, in this protocol, when a dense network automatically impacts on very high congestion, it causes time-out and will send retransmissions because of its connection mode, while UDP is a protocol intended for data transmission regardless of congestion control and error correction in a network [1] In sending packets in transmission there are several routing activities are used to run packets with correct routing. Routing is a protocol that is used to get routes or instructions from one network to another network, routing is a process where a router will choose a route or route to send or forward a packet to the destination network.

In route search, several types of topologies or designs are widely used in making routes using NS-2 simulators such as Mobile Ad-hoc Network (MANET). MANET has become popular and interesting to study because it has characteristics that are fast, saving the cost of deployment, capable of managing topology changes independently, and can be applied to emergency locations such as forest fire detection, military operations, and health monitoring [2]. MANET has three types of routing protocols including Reactive, Proactive, and Hybrid. Reactive Protocol Routing is a protocol that works on request to create new routes or route changes and Proactive Protocol Routing is a routing table, based protocol that is constantly regularly updated [3]. In Reactive Routing in the MANET topology there are several routing protocols such as AODV, AOMDV, and DSR.

The messages used in the AODV protocol are Route Request (RREQ), Route Reply (RREP), and Route Error (RERR). RREQ and RREP are route discovery, while RERR is also called route maintenance. Route discovery is initiated by spreading Route Reply (RREP). When RREP explores a node, RREP will automatically set-up the path. If a node receives RREP, then the node will send RREP again to destination sequence [4].

The Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) protocol is an extension to the AODV protocol to calculate several loop-free paths and disjoint links. The routing entry for each destination contains the next hop list along with the number of related hops. All subsequent hops have the same sequence number. This helps in tracking routes. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all paths, which is used to send the destination route ad. Each ad duplicate route received by the node defines an alternative path to destination [5]. When managing the routing protocol, MANET uses nodes as an intermediary for packet delivery. Among these nodes there are harmful ones such as Blackhole Attack which are incorporated in the Malicious node type. Nodes that carry harmful properties and behavior for the network are called malicious nodes. Malicious is able to enter the network by disguising itself or claiming to be a safe normal node to be used as a message delivery route. One of the properties of a malicious node is a blackhole attack. Blackhole itself has properties that are when there is a package or message entered and arrived at him, then the package and the message will be dropped so that the package and the message will never reach the destination. In this final project, the detection and prevention of blackhole will be carried out on the MANET network [6].

II. LITERATUR REVIEW

A. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

TCP is a connection oriented protocol. TCP provides data transmission services that are connection oriented, reliable, byte stream service. Whereas UDP provides connectionless oriented datagram delivery services, without being equipped with error detection and correction [7].

B. *Mobile Ad hoc Network (MANET)*

- Mobile Ad-Hoc Network (MANET) is a temporary wireless network that does not have a fixed infrastructure to use. MANET consists of several nodes that are able to regulate themselves without centralized control, and each node can move randomly. Therefore, the topology formed often changes because cellular nodes move independently and change their relationship to other nodes very quickly [8].
- MANET works on routable network environments above the ad-hoc network layer using the peer-to-peer method and moves on radio frequencies (30MHz - 5GHz). Thus, MANET is one of the good networks used in difficult network conditions such as military conditions, disasters, and emergency medical facilities.

C. Ad-Hoc On-Demand Distance Vector

- AODV is a reactive routing protocol that manages the latest routing information by using the route discovery procedure and an updated routing table. Knots are considered as active routes when sending, receiving, or forwarding packets. Discovery and route changes begin if there are sources who want to contact the destination or need information.
- The AODV problem is that it does not support the existence of an asymmetrical relationship and is only able to support symmetrical relationships between the source node and the destination node. The message used by the AODV protocol is:

  a. route discovery, which consists of route request (RREQ) and route reply (RREP).

  b. route maintenance, which consists of data, route update, and route error (RERR) [9].

D. Ad-Hoc On-Demand Multipath Distance

Vector AOMDV is a modification of the AODV protocol. AOMDV routing protocol is also a reactive routing protocol that uses several characteristics of proactive routing protocols. Reactive routing protocols find the path between the source and destination only when a path is needed. At AOMDV, the network is idle until a connection is needed. At that point, the network node that requires a connection broadcasts a request for connection. The message is being forwarded by another AOMDV node also recording the node that it hears from creating a temporary link explosion back to the node in need. When a link fails, routing errors are passed back to the transmitter node and then the source node selects another path stored in the memory node which is the quality and property of the AOMDV protocol [10].

B. Malicious Node

A malicious node is a node that carries a threat to a network. Malicious nodes move randomly to attack a network that exists and can enter into the network because of its nature that resembles normal nodes in general. This causes other nodes to assume that the malicious node is a safe node, even though it contains dangerous elements. Blackhole Attack

Malicious nodes act like a blackhole. Specifically, the malicious node will send fake RREP to all RREQs and pretend to get a route to be sent to the destination node. After receiving the data package, the malicious node will discard it.

C. Quality of Service (QoS)

QoS in telecommunications systems is related to network performance of the underlying routing system. QoS is also defined as the collective effect of service performance that determines the level of satisfaction of service users [11].

a) Throughput
Throughput is the number of bytes received at certain intervals in bytes per second which is the condition of the actual data rate in a network.

b) Packet Loss
Packet loss is a packet of data lost from the entire packet of data sent during the process of sending from the client to the server and back to the client during that time period. In general, packet loss occurs due to limited buffers and wrong packet sequences.

c) Jitter
Jitter is a variation of delay, which is the difference in the interval of arrival time between packages at the destination terminal. Jitter is influenced by variations in traffic load and the magnitude of collisions between packets (congestion) in the network.

D. Energy

Energy is the ability to do business. Energy is an eternal quantity, meaning that energy cannot be created and destroyed, but can be changed from one form to another.

III. PROBLEM STATEMENT

In getting the results of the simulation based on throughput, packet loss, and jitter parameters there are several steps that must be taken, namely to create a network simulation scenario by using the Version 2.35 all-in-one Network Simulation (NS2) application that is used as the compiler syntax that has been created in the file with extension .tcl which contains input node settings and the distance used in the scenario required during the simulation.The scenarios carried out using the Mobile Ad-Hoc Network (MANET) topology with different number of nodes and the number of Malicious Node in different simulations. According to Setijadi (2018) the number has an important role in the results of the Throughput, Packet Loss, and Jitter parameters.In addition to using differences in the number of nodes and the number of malicious nodes, in this study also used two routing protocols as packet senders between nodes in a simulation scenario. The routing protocol used is AODV and AOMDV (Reactive Routing), and uses two packet transmissions namely TCP (Transmission Control Protocol) and UDP (User Diagram Protocol) and the presence of a disorder using Malicious Node (Blackhole Attack).

The use of Mobile Ad-Hoc Network (MANET) topology is due to the study of Neetha Paulose and Neethu Paulose in 2016, examining the value of Throughput and Packet Loss using AODV and AOMDV routing protocols and using only one packet transmission, namely UDP in Manet Topology. Therefore, in this study we will use the MANET topology as a network that is used to find results based on Throughtput, Packet Loss, and Jitter parameters

IV. RESEARCH MOTIVATION

In the last few years the development of wireless technology nodes is increasingly advanced. The development of MANET (Mobile Ad-Hoc Network) is one of the wireless topologies that has become popular and interesting to be examined because it has characteristics that are fast, able to manage topological changes in a bath, save the cost of distribution. In previous studies several journals only used one packet transmission and several routing protocols, and in my study I used two packet transitions and two routing protocols and there was involvement of a malicious node, namely a blackhole attack. The purpose of this research is to find out the results of the comparison of the performance of AODV and AOMDV protocols with TCP and UDP on MANET (Mobile Ad-Hoc Network) using Malicious Node (Blackhole Attack).

But in several studies to find the results of the data using only one packet transmission using the MANET topology and not using other topologies. Referring to the research conducted by Neetha Paulose and Neethu Paulose in 2016, we have examined the value of Throughput and Packet Loss using the AODV and AOMDV routing protocols and only use one packet transmission, namely UDP in Manet Topology. Based on the results of their research, it can be concluded that the AOMDV routing protocol is superior in package delivery and reduction in the risk of packet loss while AODV cannot provide the best results on package delivery.

Other similar research is that in the research of Neetika Bhardwaj and Rajdeep Singh conducted the results of UDP packet transmission based on the AOMDV routing protocol in the presence of Malicious Node interference, namely Blackhole Attack. In this study MANET topology was used as a cross-network in the simulation. Looking at the two types of previous research, in this study we will compare the performance of two AOMDV and AODV routing protocols on TCP and UDP and the existence of a malicious node (Blackhole Attack) to find out the results based on Throughput, Packet Loss, and Jitter parameters.

V. METHOD

The method used was a simulation. It started from primary data collection and continues with a literature study of some literature related to research along with books that discuss research. Then proceed with the simulation method, Fig1 is the framework of this study.

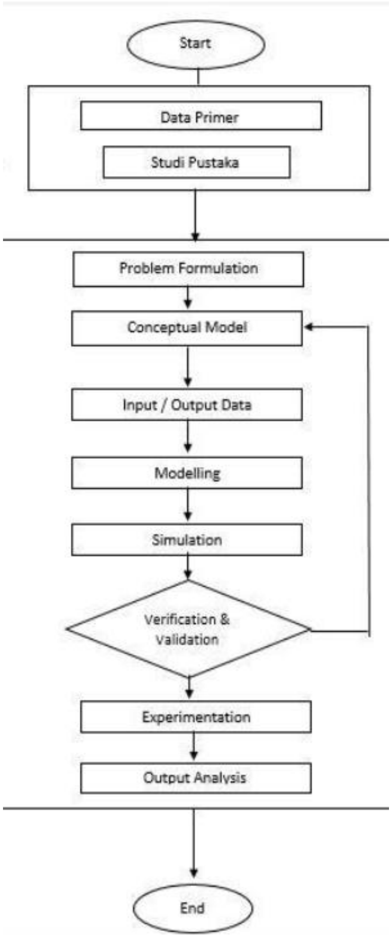


Figure 1 Framework Design

A. Problem Formulation

This study will evaluate and compare the performance of MANET energy efficient from two routing protocols namely AODV and AOMDV using different nodes and malicious nodes to help produce comparisons issued in QoS in the form of throughput, packet loss, and jitter to know the impact of the malicious node is in the MANET topology.

B. Conceptual Model

At this stage the writer configures MANET and will use a random way point system, where the node will be placed randomly wirelessly. The router role that will be used is the sender /source (sender), receiver (receiver), and attacker/malicious (attacker). The simulation is designed using NS2 as a compiler, then the simulation results will be released using NAM and will evaluate the results based on files that have the extension .tr / .trace.

The simulation process is based on two conditions, namely changes in nodes and malicious nodes. The process of drawing the packet used is the TCP and UDP transmission protocol for 300 seconds or 5 minutes.

C. Input/Output Data

a) Input

The following are some of the input attributes used in this simulation, namely:

- Node is a point where a device is on a network. In MANET, each node must have coordinates based on the X and Y axes. Because it uses the MANET routing protocol, these nodes can be randomly moved from point to point. This simulation uses nodes 50 and 100 and malicious nodes 1 and 10.
- Role This simulation will use three roles, namely: (i) the source / sender whose job is to send packets to the receiver, (ii) the receiver (receiver) whose task is to receive packets sent by the source / sender, and (iii) malicious nodes whose duty is to disrupt and disrupt the process of sending the packet by making all the packets that have been sent by the sender.
- Packetsize is a quantity that shows the number of units of data to be sent in one communication time. The number of packetsizes used in this simulation is 512 bytes.

b) Output

The following are some of the output attributes used in this simulation, namely:

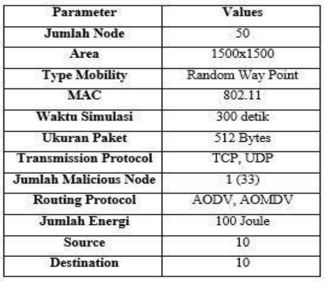
- Throughput is used to measure the speed of sending packets in AODV and AOMDV routing protocols with malicious nodes.
- Packet Loss is used to measure the number of packets received, in the form of a percentage.
- Jitter is used to measure the delay of a packet sent from the source / sender to the receiver.

D. Modeling

At this stage the author will divide the simulation into several scenarios, then compare the performance of the QoS and energy results from TCP and UDP in the AODV and AOMDV routing protocols in each scenario that has been done. The scenario created as follows:

a) Scenario 1

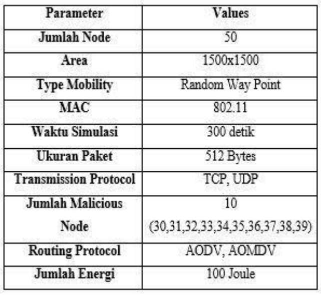
TABLE I. SCENARIO 1



Parameter	Values
Jumlah Node	50
Area	1500x1500
Type Mobility	Random Way Point
MAC	802.11
Waktu Simulasi	300 detik
Ukuran Paket	512 Bytes
Transmission Protocol	TCP, UDP
Jumlah Malicious Node	1 (33)
Routing Protocol	AODV, AOMDV
Jumlah Energi	100 Joule
Source	10
Destination	10

b) Scenario 2

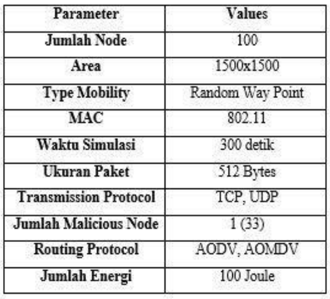
TABLE II. SCENARIO 2



Parameter	Values
Jumlah Node	50
Area	1500x1500
Type Mobility	Random Way Point
MAC	802.11
Waktu Simulasi	300 detik
Ukuran Paket	512 Bytes
Transmission Protocol	TCP, UDP
Jumlah Malicious Node	10 (30,31,32,33,34,35,36,37,38,39)
Routing Protocol	AODV, AOMDV
Jumlah Energi	100 Joule

c) Scenario 3

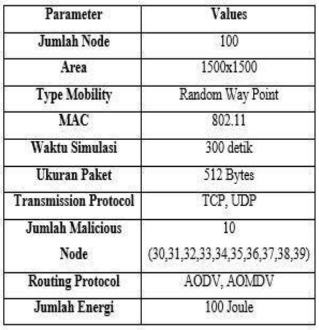
TABLE III. SCENARIO 3



Parameter	Values
Jumlah Node	100
Area	1500x1500
Type Mobility	Random Way Point
MAC	802.11
Waktu Simulasi	300 detik
Ukuran Paket	512 Bytes
Transmission Protocol	TCP, UDP
Jumlah Malicious Node	1 (33)
Routing Protocol	AODV, AOMDV
Jumlah Energi	100 Joule

d) Scenario 4

TABLE IV. SCENARIO 4



Parameter	Values
Jumlah Node	100
Area	1500x1500
Type Mobility	Random Way Point
MAC	802.11
Waktu Simulasi	300 detik
Ukuran Paket	512 Bytes
Transmission Protocol	TCP, UDP
Jumlah Malicious Node	10 (30,31,32,33,34,35,36,37,38,39)
Routing Protocol	AODV, AOMDV
Jumlah Energi	100 Joule

E. Simulation

At this stage the author simulates using the Ubuntu 16.04 operating system. Simulations are carried out with a number of 2.35 all-inone NS2 (Network Simulation 2) applications that are used as compiler syntax that has been created in the .tcl format file that contains input node settings and commands performed during the simulation. When the simulation of the .tcl format file is complete, the simulation will issue the file type .nam and .tr.

The NAM application (Network Animator) will run a .nam file to run animations during the simulation. The author will also use the awk script to find the results of the parameters throughput, packet loss, jitter and energy taken from the .tr file and will be displayed in the form of tables and graphs.

F. Verification and Validation

This stage is the stage to verify and validate the scenario that has been made. The scenario will be tested to find out if the simulation that has been carried out has gone well according to the stipulated conditions.

a) Simulation Configuration Testing

The test uses the NS2 application by compiling the tcl file containing the simulation configuration. Compilation is done with the "$ ns <tcl filename>" command. If the compilation is successful, it will produce 2 files in the form of .tr and .nam.

b) Testing Routing Protocol

Testing is done to check the AODV and AOMDV routing protocol is running properly or not. Testing is done by running a .nam file obtained from running the .tcl file, using the "$ nam <file .nam>" command and seeing whether source and destination can send the packet.

c) Testing UDP and TCP Packages

Tests are carried out to check whether the delivered UDP package can run properly or not. Testing is done by calculating the value of throughput, packet loss, and jitter taken from the .tr file data.

d) Perfoma Test using Malicious Node Network

This test is done to check whether the UDP and TCP packets that are sent can run well. Testing is done by calculating the value of throughput, packet loss, and jitter from the .tr file.

VI. RESULT AND DISCUSSION

A. Scenario 1

- *THROUGHPUT*

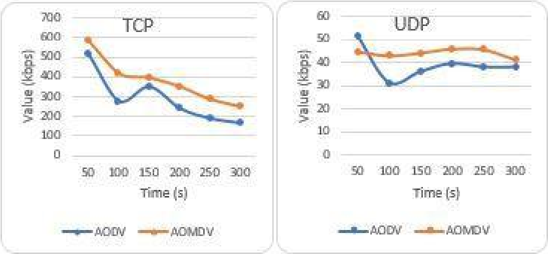


Figure 2 *Throughput* TCP and UDP

In the TCP throughput graph, the maximum value for AODV is 516.09 kbit / s when the simulation time is 50 seconds and for AOMDV is 584.01 kbit / s during the simulation time of 50 seconds. Whereas for UDP throughput the maximum value for AODV is 51.89 kbit / s when the simulation time is 50 seconds and for AOMDV is 45.98 kbit / s at simulation time of 250 seconds

- *PACKET LOSS*

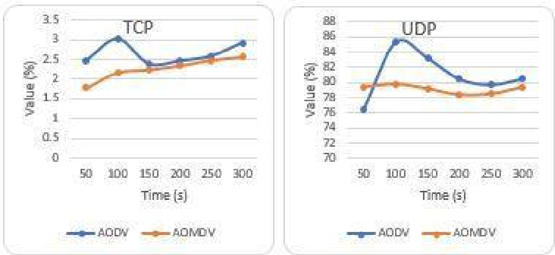


Figure 3 *Packet Loss* TCP and UDP

In the TCP graphics packet loss the maximum value for AODV is 3.01% when the simulation time is 100 seconds and for AOMDV it is 2.56% during the simulation time of 300 seconds. Whereas in UDP packet loss the maximum value for AODV is 85.35% when the simulation time is 100 seconds and for AOMDV is 79.78% when the simulation time is 100 seconds.

- *Jitter*

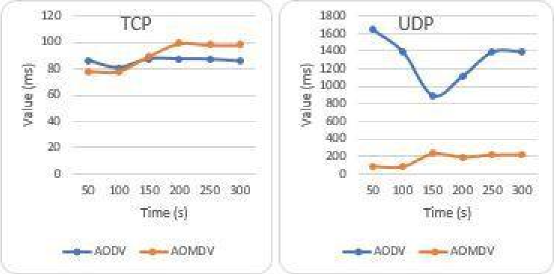


Figure 4 *Jitter* TCP and UDP

On the TCP jitter graph, the maximum value for AODV is 87.43 ms when the simulation time is 150 seconds and for AOMDV is 99.15 ms when the simulation time is 200 seconds. Whereas in UDP jitter the maximum value for AODV is 1647.58 ms when the simulation time is 50 seconds and for AOMDV is 231,378 ms at the simulation time of 150 seconds.

B. Scenario 2

- *THROUGHPUT*

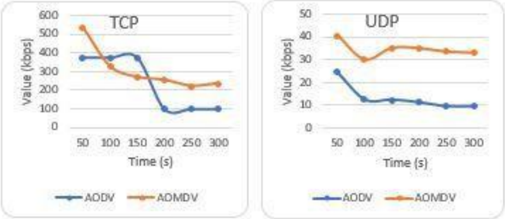


Figure 5 *Throughput* TCP and UDP

In the TCP throughput graph, the maximum value for AODV is 373.05 kbit / s during the simulation time of 150 seconds and for AOMDV is 535.79 kbit / s during the simulation time of 50 seconds. Whereas in UDP throughput the maximum value for AODV is 24.64 kbit / s when the simulation time is 50 seconds and for AOMDV is 40.59 kbit / s during the simulation time of 50 seconds.

- *PACKET LOSS*

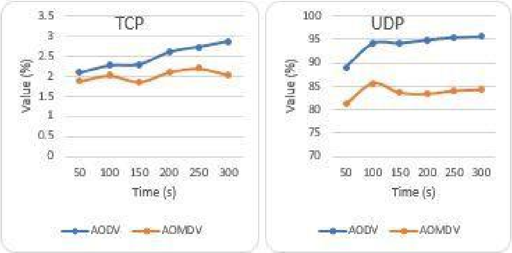


Figure 6 *Packet Loss* TCP UDP

In the TCP graphics packet loss the maximum value for AODV is 2.87% when the simulation time is 300 seconds and for AOMDV it is 2.2% during the simulation time of 250 seconds. Whereas in UDP packet loss the maximum value for AODV is 95.62% when the simulation time is 300 seconds and for AOMDV is 85.66% when the simulation time is 100 seconds.

- *Jitter*

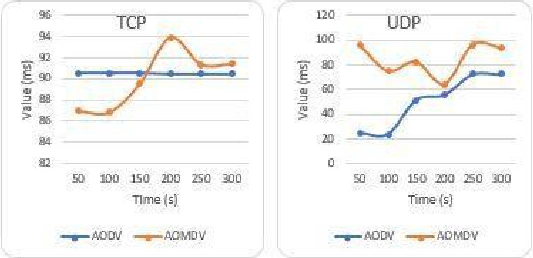


Figure 7 *Jitter* TCP and UDP

On the TCP jitter graph, the maximum value for AODV is 90.5604 ms when the simulation time is 150 seconds and for AOMDV it is 91.3996 ms during the simulation time of 300 seconds. Whereas in UDP jitter the maximum value for AODV is 72.3869 ms when the simulation time is 300 seconds and for AOMDV is 95.9961 ms at simulation time of 250 seconds.

C. Scenario 3

- *THROUGHPUT*

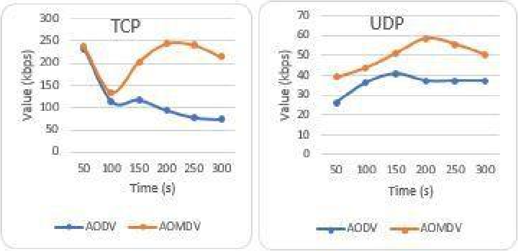


Figure 8 *Throughput* TCP and UDP

In the TCP throughput graph, the maximum value for AODV is 232.89 kbit / s when the simulation time is 50 seconds and for AOMDV is 243.89 kbit / s during the simulation time of 150 seconds. While the UDP throughput obtained the maximum value for AODV is 41.09 kbit / s at simulation time of 150 seconds and for AOMDV is 58.71 kbit / s during the simulation time of 200 seconds.

- *PACKET LOSS*

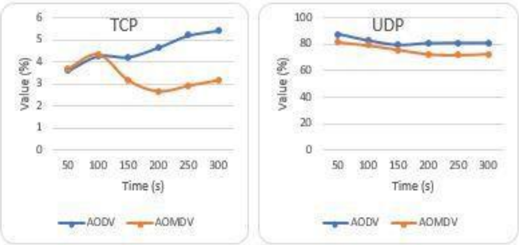


Figure 9 *Packet Loss* TCP and UDP

In the TCP graphics packet loss the maximum value for AODV is 5.43% when the simulation time is 300 seconds and for AOMDV is 4.36% at simulation time of 100 seconds. Whereas in UDP packet loss the maximum value for AODV is 87.65% when the simulation time is 50 seconds and for AOMDV is 81.83% when the simulation time is 50 seconds.

- *JITTER*

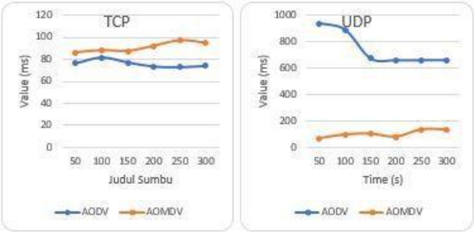


Figure 10 *Jitter* TCP and UDP

On the TCP jitter graph, the maximum value for AODV is 81.79 ms when the simulation time is 100 seconds and for AOMDV is 97.11 ms during the simulation time of 250 seconds. Whereas in UDP jitter the maximum value for AODV is 937,163 ms when the simulation time is 50 seconds and for AOMDV is 137.67 ms when the simulation time is 250 seconds.

D. Scenario 4

- *THROUGHPUT*

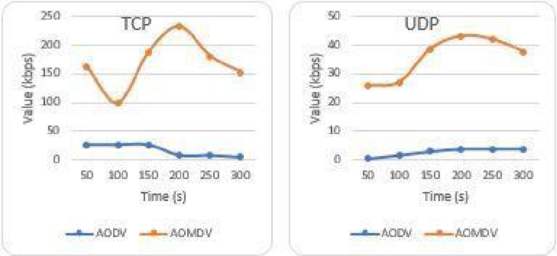


Figure 11 *Throughput* TCP and UDP

In the TCP throughput graph, the maximum value for AODV is 516.09 kbit / s when the simulation time is 50 seconds and for AOMDV is 584.01 kbit / s during the simulation time of 50 seconds. Whereas for UDP throughput the maximum value for AODV is 51.89 kbit / s when the simulation time is 50 seconds and for AOMDV is 45.98 kbit / s during simulation time of 250 seconds.

- PACKET LOSS

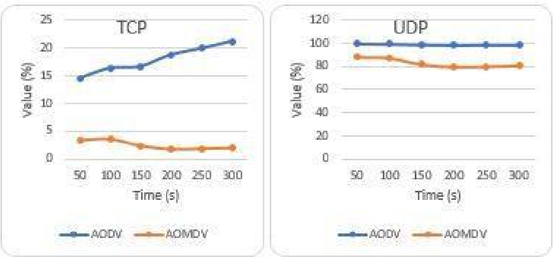


Figure 12 *Packet Loss* TCP and UDP

In the TCP packet loss graph, the maximum value for AODV is 21.19% when the simulation time is 300 seconds and for AOMDV it is 3.68% when the simulation time is 100 seconds. Whereas in UDP packet loss the maximum value for AODV is 99.38% when the simulation time is 100 seconds and for AOMDV is 88.05% when the simulation time is 50 seconds.

- *JITTER*

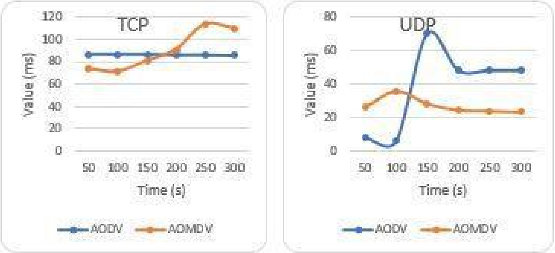


Figure 13 *Jitter* TCP and UDP

On the TCP jitter graph, the maximum value for AODV is 86.14 ms when the simulation time is 150 seconds and for AOMDV is 113.1 ms when the simulation time is 250 seconds. Whereas in UDP jitter the maximum value for AODV is 48.3526 ms when the simulation time is 300 seconds and for AOMDV is 35.3056 ms at simulation time of 100 seconds.

VII. CONCLUSIONs

In the evaluation results, the author obtained the results that the Routing Protocol AODV and AOMDV on TCP and UDP had very different transmission differences. On the results of AOMDV Throughput on TCP and UDP in 4 scenarios have a higher average value due to the dominant function of AOMDV which can find the best route and run RREP on many routes, in AODV predominantly have low results because in the simulation scenario using a malicious node so the routing of data can be lost and cannot have another route back up. On the results of Packet Loss AOMDV TCP has a packet loss value less than TCP AODV because it has multi routing when there is a problem sending, whereas for UDP the AODV value has a lot of packet loss because it has 1 RREP and AOMDV routes UDP has several RREP routes so that the packet can be realized better. In the Jitter Result the highest value is obtained on AODV and AOMDV Protocol Routing on TCP because it has a flow control function that can set the trajectory on the route so that congestion does not occur. And in UDP AODV in scenarios 1 and 3 have a very high value due to malicious used, different in AODV scenarios 2 and 4 which have as many as 10 malicious nodes, and for malicious nodes the greater the number of malicious nodes in a network will cause the routing process to be carried out often because the number of packets is removed by the malicious node.

From the Routing Simulation Results AODV and AOMDV protocols on TCP have good results because the functions of TCP performance prioritize security and the success of packets sent and received, although the malfunction of the malicious node TCP works properly so that the most dominant risk on TCP is packet delay because it often occurs re-sending or running out of energy at each Node which causes the packet to stop on the road.

From the results of the routing simulation, the AODV and AOMDV protocols at UDP have good results in terms of speed because the original UDP function is sending packets regardless of the risks involved in sending, the AODV and AOMDV results are not too different but the UDP energy quality is more prominent because shipping that is done directly on the delivery without thinking about the package condition.

So, it can be concluded from Routing AODV and AOMDV protocols on TCP and UDP packet transmissions have their respective uses, some are useful for securing data while having use in speed of transmission, so for selection of transmission and routing protocols needed depending on what is user needs.

REFERENCES

[1] Mardiana, Y., & Sahputra, J. (2017). Analisa Performansi Protokol TCP, UDP, dan SCTP. Jurnal Media Infotama, 13(2), 73–84.

[2] Setijadi, E., Purnama, I. K. E., & Purnomo, M. H. (2018). Analisis Kinerja Protokol Routing Reaktif dan Proaktif pada MANET Menggunakan NS2, 7(2), 138–143.

[3] *Ibid.*

[4] Purba, D. U., Primananda, R., & Amron, K. (2018). Analisis Kinerja Protokol Ad Hoc On-Demand Distance Vector (AODV) dan Fisheye State Routing (FSR) pada Mobile Ad Hoc Network. Pengembangan Teknologi Informasi Dn Ilmu Komputer, 2(7), 2626–2634.

[5] Dahiya, P., Madan, G., Gupta, R. (2014). Performance Evaluation of AODV and AOMDV On the Basis of Throughput, 3(9), 277-283.

[6] Wicaksono Setyo, S. R. (2017). *Rekayasa Perangkat Lunak.*

[7] Sofana, I. (2013). Membangun Jaringan Komputer.

[8] Wicaksono Setyo, S. R. (2017). Rekayasa Perangkat Lunak.

[9] C. Perkins. (n.d.). Ad-hoc On-Demand Distance Vector (AODV) Routing.

[10] Saini, D., & Saini, G. L. (2017). Art20173387, 6(5), 1216–1222.

[11] Paul, S., & Pandit, M. K. (2018). A QoSenhanced intelligent stochastic real-time packet scheduler for multimedia {IP} traffic. Multimedia Tools Appl., 77(10), 12725–12748. https://doi.org/10.1007/s11042-017-4912-6