Performance Evaluation of AODV and AOMDV Routing Protocol on Rushing Attack for Wireless Mesh Network

Siti Ummi Masruroh, Muhammad Irian Iqbal and Nashrul Hakiem
Department of Informatics, Faculty of Science and Technology, UIN Jakarta.
ummi.masruroh@uinjkt.ac.id

***Abstract*—Wireless LAN (WLAN) technology is becoming increasingly popular as an option to provide wireless internet access in corporate, campus, residential, public space, and others. Wireless Mesh Network (WMN), as one of the innovations of WLAN technology offers a unique solution as it can effectively and efficiently replace or enrich the capabilities of both the existing wired and wireless-based internet network infrastructure. This is because it can cover wider and difficult to reach service areas without ignoring security, mobility, and Quality of Service (QoS). This paper evaluated the impact of AODV and AOMDV routing protocol performance when under attack by Rushing Attack. This simulation used 49 and 100 nodes and Network Simulator 2 (NS2) and Network Animator (NAM) to evaluate the performance and the QoS parameters, namely the throughput, packet delivery ratio, packet drop rate, and end-to-end delay. The results from the trace file were derived from the evaluation of QoS. Based on the evaluation, it was found that AOMDV produces better performance than AODV. AOMDV has a higher performance evaluation of several Kbps because AOMDV has many backup paths, if the path used to send packets from source to destination is no longer efficient.**

***Index Terms*—AODV; AOMDV; Rushing Attack; Wireless Mesh Network.**

I. INTRODUCTION

Wireless Mesh Networks (WMNs) is a technology that is developing and making a significant progress in the field of wireless networks in recent years. Mesh networks are capable of rapid deployment and reconfiguration and this provides benefits such as low up-front costs, simplicity of network configuration, easier and faster network maintenance, broadband capability, and reliable service coverage. It usually consists of a mesh router and a mesh client, where each node can operate as a host and router. Mesh routers generally have minimal mobility in the mesh network and form the backbone of WMNs. Clients can be stationary or cellular and can form self-managed ad hoc networks that can access services by sending requests to a wireless backbone network [1].

Distance Vector (AODV) routing protocol uses an on-demand approach to find a route; that is, a route is created only if it is needed by the source node to send data packets. This uses the destination serial number to identify the latest path. In AODV, source nodes and intermediary nodes store next-hop information that corresponds to each stream for data packet transmission [2].

Ad-Hoc On-Demand Multipath Distance Vector (AOMDV) Routing Protocol is a development of the AODV protocol. The number of routes found each time searching for a route is the main difference between AODV and AOMDV. Unlike AODV that selects only one RREP when searching routes, AOMDV considers each RREP by the original node so that several paths can be found in one route search. Thus, if a route fails during the transmission, it can be diverted to another route [3].

We compare the performance of the two AODVs and AOMDV routing protocols because they have differences in the number of routes found in each route search process, and we use several parameters including throughput, packet delivery ratio (PDR), Packet Drop Rate, end-to-end delay to test its performance.

Rushing attacks are zero delay attacks and are effective when the attacker is near to the source or destination node. Request routing protocols, such as AOMDV are more vulnerable to this attack, because every time the source node floods the packet request route in the network, the malicious node receives the packet request route and sends without hop-count every update and delay in the network. They are dropped every time the node receives the source request packages. After that the nodes received packets from attackers and threats that currently receive packets, such as duplicate packages. Thus, the malicious included in the route will be active and interfere with the data forwarding phase. Rushing attacks can take place at the source or the destination or in the center [3].

II. PROBLEM STATEMENT

Referring to the related previous works [1], evaluation results of AODV and AOMDV routing protocols are QoS parameters, namely packet delivery ratio, normalized routing overhead, and end-to-end delay on mesh networks. But in this study only one node variation without the existence of a malicious node will be used. Further, a comparison of the on-demand routing protocols between AODV and AOMD will be conducted [4]. Although the evaluation results of the AODV and AOMDV routing protocols commonly use QoS parameters, namely the throughput and packet loss on the MANET network, this study used only one node variation without the existence of a malicious node. There is also research about AOMDV performance evaluation when attacked with a rushing attack on VANET [3].

III. MOTIVATION

Internet access has become one of the most basic needs of today's society, especially for Millennials. Wireless LAN

(WLAN) technology is one of the choices in providing wireless internet access to corporate, campus, residential, public space, etc. There is a lot of research to develop and see the results of the performance of a network to enjoy internet services without thinking about the adverse impacts or expensive costs.

To determine the performance of an internet network, there are several criteria which are usually often referred to as Quality of Service (QoS). According to Rahmad Saleh Lubis (2014) [5], quality of service is a measurement method of how well is the network, and it is an attempt to define the characteristics and properties of testing service to get the results of the QoS.

With respect to the choice of the attack type in the form of a rushing attack, Ratnasih (2018) highlighted that rushing the attack that makes packets through nodes affected by malicious nodes will be discarded or duplicated quickly with higher transmission to disrupt the network and get more forward access compared to other nodes [3]. Therefore, the writer tries to compare the performance of two routing protocols, namely AODV and AOMDV when both are exposed to rushing attacks on the wireless mesh network. With packet delivery ratio parameters, throughput, end-to-end delay, and packet drop rate.

IV. RESEARCH METHOD

The method used in this research is a simulation method, Figure 1 is the research flow that starts from literature studies, similar research studies, identification of problems in which data are collected from several literature studies related to research along with research books. Then, it is proceeded with the simulation method. The research flow of this research is shown below.

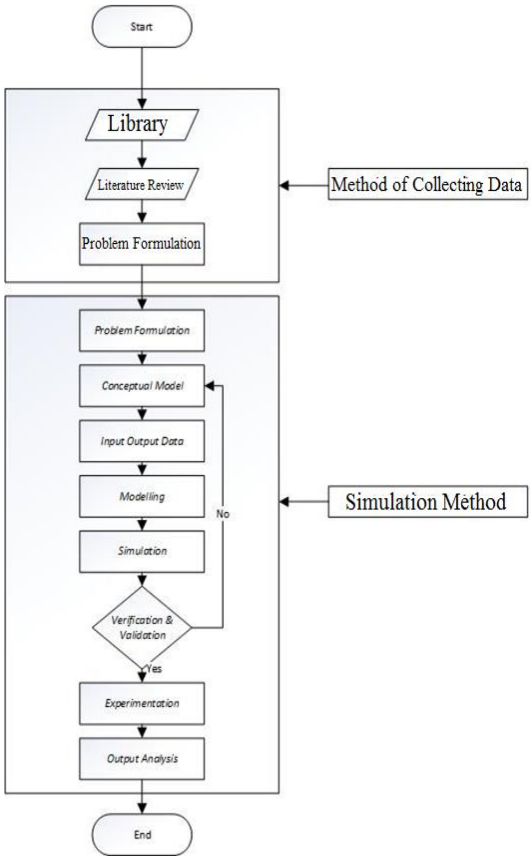

Figure 1: Research flow

The simulation method adopted in this study is described below.

A. Problem Formulation

To determine the impact caused by the malicious node such as the rushing attack on the Wireless Mesh Network (WMN). Performance evaluation of the routing protocol based on the Quality of Service (QoS) parameter is needed.

B. Conceptual Model

In this phase, the author configures the Wireless Mesh Network (WMN). Specifically, the author configured the static node of the mesh topology to fixed wireless. The role of the router that will be used is the sender, the receiver, and the attacker. The simulation was designed and compiled using Network Simulator 2 (NS2) as a compiler. Then, the simulation was run using Network Animator (NAM), and evaluated based on the .tr file.

C. Input / Output Data

1) Input

The followings are some of the input attributes used in this simulation:

- Node: The node is a point where the location of a device is in the network. Each node must have coordinates based on the x and y axes. In the Wireless Mesh Network (WMN) the node is fixed (static) so that its position cannot be moved. The number of nodes used in this simulation is 49 and 100 nodes, and there are three malicious nodes.
- Role: The role is to recognize nodes with their respective tasks. In this simulation, it uses three roles, namely the source/sender (sending packets to the destination), destination (receiving packages from destination), and attackers (attacking the package delivery process).
- Packet Size: Packet size is a quantity that shows the number of units of data to be sent during communication time. The number of packet sizes used in this simulation is 1024 bytes.

2) Output

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

- Throughput: Throughput is the total number of data packets that are successfully received in units of time and it describes the condition of the data speed in a network. The higher the value of throughput produced, the better the performance of the routing protocol[6].

Table 1
Standardization of Throughput

Category	Throughput
Very Good	100 %
Good	75 %
Medium	50 %
Bad	< 25 %

The throughput value is derived using equation (1) [7].

$$\text{Throughput} = \frac{\text{No. of bytes recieved} \times 8}{\text{Simulation time} \times 1000} \text{Kbps} \quad (1)$$

- Packet Delivery Ratio (PDR): PDR is a comparison of the number of packets successfully received by the destination node with the total packet sent by the source node. PDR is one of the QoS parameters that shows the success rate of a routing protocol [6]. Table 2 shows the value of the PDR category [5].

Table 2
Standardization of PDR

Category	PDR
Very Good	100 %
Good	97 %
Medium	85 %
Bad	75 %

The PDR value is measured using equation 2 [7].

$$\text{PDR} = \frac{\text{No. of packet recieved}}{\text{No. of packet sent}} \times 100 \quad (2)$$

- Packet Drop Rate: Packet drop rate is measured as the percentage of packets lost in connection with packets sent between sources to destination [6]. Table 3 shows the value of the packet drop rate category [8].

Table 3
Standardization of Packet Drop Rate

Category	Packet Loss
Very Good	0 %
Good	3 %
Medium	15 %
Bad	25 %

The packet drop rate value is measuring using equation 3 [9].

$$\frac{(\text{Paket data dikirim} - \text{Paket data diterima})}{\text{paket data yang diirim}} x\ 100\% \quad (3)$$

- End-to-end Delay: Delay is the time delay for all packets that are successfully sent from the source node to the destination node [6]. Table 4 shows the value of the delay category.

Table 4
Standardization of Delay

Category	Delay
Very Good	< 150 ms
Good	150 s/d 300 ms
Medium	300 s/d 450 ms
Bad	> 450 ms

The delay value is measured using equation 4 [7].

$$\text{End to End Delay} = \frac{\sum(\text{arrive time} - \text{send time})}{\sum \text{no. of connections}} \quad (4)$$

D. Modeling

In the simulation design discussed earlier, the author has designed the simulation as follows:

Table 5
Simulation Scenario

Parameters	Value
Number of Nodes	49 & 100
Area	1.100 m x 600 m
Type Mobility	Mesh
MAC	802.11
Simulation Time	100 seconds
Routing Protocol	AODV
Traffic Type	CBR
Transmission Protocol	UDP
Packet Size	1024 bytes
Malicious node	3
Malicious Initiate Time	0 second

There are four scenarios in this simulation. Each node will be configured using AODV routing protocol (scenario 1 & 2) and AOMDV routing protocol (scenario 3 & 4) with a size of area 1,100 m x 600 m, using number of nodes 49 and 100 (7^2 & 10^2) pieces. The type of traffic used is CBR uses the UDP transmission protocol with a package size of 1024 bytes. The simulation takes 100 seconds. Each scenario gives the same number and location of the malicious node.

E. Simulation

In this phase, the author used the Ubuntu Linux operating system 16.04. The research was carried out using NS2 version 2.35 all-in-one application, which functions to compile syntax with extension .tcl containing the input needed along with the setting of node activity during the simulation. The compiled results are files with extension .nam and .tr.

F. Verification and Validation

This phase is a step to verify and validate the previous simulation. Each scenario in the previous phase was tested to find out whether the simulation has run according to what was determined in the Conceptual Model, Data Input / Output, and Modeling phases.

G. Experimentation

At this phase, each scenario that has been previously designed was carried out by following the objectives specified in the conceptual model phase.

H. Output Analysis

In this phase, all simulation results were recorded in a table form. These results are outputs of the performance of the routing protocol results of each simulation by including throughput parameters, packet delivery ratio, packet drop rate, and end-to-end delay. Testing was done by analyzing trace files using the .awk script.

V. Result And Discussion

A. Results

Table 6 and 7 show the results of comparison about the Quality of Service on AODV and AOMDV. The following

result is displayed using blue marks for the nodes with 49 pieces and yellow marks for the nodes with 100 pieces:

Table 6
The Results of the AODV Routing Protocol Performance

AODV				
Time (s)				
20	40	60	80	100
Throughput (Kbps)				
87,03	90,53	91,65	92,21	92,54
88,57	91,28	92,14	92,57	92,83
Packet Delivery Ratio (%)				
84,87	88,52	89,70	90,28	90,63
86,55	89,34	90,24	90,69	90,95
Packet Drop Rate (%)				
15,13	11,48	10,30	9,72	9,37
13,45	10,66	9,76	9,31	9,05
End-to-End Delay (ms)				
2235,33	4234,51	6235,33	8235,33	10235,30
2705,17	4705,95	6705,98	8705,95	10705,9

Table 7
The Results of the AOMDV Routing Protocol Performance

AOMDV				
Time (s)				
20	40	60	80	100
Throughput (Kbps)				
101,78	100,43	100,55	100,92	101,03
101,35	101,69	101,79	101,84	101,56
Packet Delivery Ratio (%)				
99,16	98,16	98,51	98,89	99,03
98,74	99,39	99,73	99,70	99,52
Packet Drop Rate (%)				
0,84	1,84	1,49	1,11	0,97
1,26	0,61	0,27	0,30	0,48
End-to-End Delay (ms)				
121,231	121,010	121,070	120,355	120,214
271,889	272,378	271,321	272,908	271,144

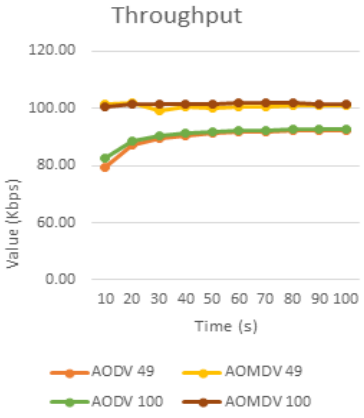

Figure 2: Graph of throughput comparison between AODV and AOMDV

In Figure 2, the graph shows a comparison of the throughput value between AODV and AOMDV. The greater the throughput value of a network, the more number of packets that can be sent to the destination. On variations in the number of 49 nodes, AOMDV has a better throughput value compared to AODV.

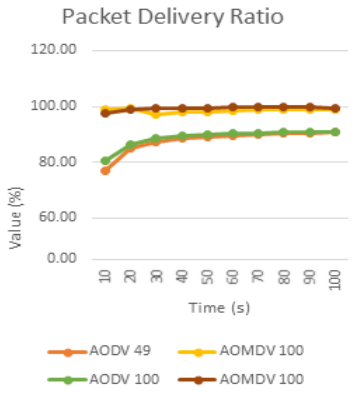

Figure 3: Graph of PDR Comparison between AODV and AOMDV

In Figure 3, the graph shows a comparison of the PDR value between AODV and AOMDV. The greater the PDR value of a network, the more number of packets that are successfully sent. On variations in the number of 49 nodes, AOMDV has a better PDR value than AODV.

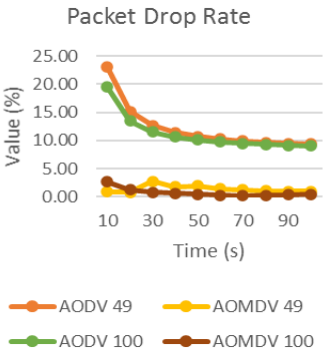

Figure 4: Graph of packet drop rate comparison between AODV and AOMDV

In Figure 4, the graph shows a comparison of the value of the packet drop rate between AODV and AOMDV. The greater the value of the packet drop rate, the more number of packets that are not sent successfully. On variations in the number of 49 nodes, AOMDV has a better packet drop rate than using AODV.

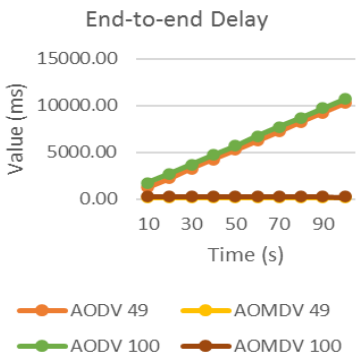

Figure 5: Graph of delay comparison between AODV and AOMDV

In Figure 5, the graph shows the comparison of end-to-end delay values between AODV and AOMDV. The greater the end-to-end delay value of a network, the longer the packet reaches its destination. On variations in the number of 49 nodes, AOMDV has a better end-to-end delay compared to AODV.

B. Discussion

This study relate to the previous works [4] that discussed routing solutions for AODV and AOMDV protocols on Mobile Ad-Hoc Network that use parameters throughput and packet loss. Based on the results, it can be concluded that the AOMDV routing protocol is superior in terms of packet delivery speed, throughput, and theft of the average end-to-end delay.

A comparison of two on-demand routing protocols, AODV and AOMDV has been conducted. AODV is the most basic on-demand routing protocol, and most of the routing protocols are the enhanced or modified version of AODV. The Ad Hoc On-demand Distance Vector (AODV) routing scheme is a widely used routing technique in ad hoc networks due to its low routing traffic overhead. However, the performance of the minimum hop routing used by AODV degrades significantly when the underlying system has routes that have high throughput and hop count. Ad hoc On-demand Multipath Distance Vector (AOMDV) is the enhanced version of AODV protocol, it belongs to on-demand and reactive routing protocol of ad-hoc wireless networks. The main goal is to compute multiple loop-free and link-disjoint paths between source and destination pair. The merit of AOMDV is estimated in terms of the increased packet delivery ratio, throughput, and reduced average end-to-end delay and normalized control overhead [4].

The choice of the malicious node, which is a rushing attack has its reasons. Rushing attacks make packets through nodes that are affected by malicious nodes need to be discarded or duplicated quickly with higher transmission to disrupt the network and get more forward access, when compared to other nodes [3].

When attacked by rushing attacks, any changes in the transmission line or packets that fail to be sent affect the results of the routing protocol performance evaluation.

In the results of throughput comparison, AOMDV has a higher performance evaluation of several Kbps because AOMDV has many backup paths, if one time the path that is being used to send packets from source to destination is no longer efficient.

Several factors affect the performance of a routing protocol, one of which is a long processing time. It can be seen from tables and graphs that the longer the time the simulation runs on the AODV routing protocol the resultant delay increasing. While at AOMDV, most of the delay generated was greater than the previous second average.

VI. CONCLUSION

Based on the simulation conducted by the author, the authors conclude that between the two routing protocols AODV and AOMDV, when attacked by the malicious nodes such as a rushing attack with both the number of nodes is 49 or 100. The AOMDV routing protocol is better than AODV. With the category results of a **medium** evaluation of the AODV routing protocol and **good** up to **very good** for the AOMDV routing protocol. Also, the AOMDV routing protocol has a better throughput value than AODV, especially in mesh networks that have several 100 nodes. Likewise, with the end-to-end delay parameters, the AOMDV routing protocol far outperforms the AODV routing protocol performance **very well** on 49 nodes and is **good** for 100 nodes. However, the performance of the AODV routing protocol itself in end-to-end delay parameters is quite **bad**.

Referring to the conclusion above, the AOMDV routing protocol has a better performance based on throughput, packet delivery ratio, packet drop rate, and end-to-end delay parameters when attacked by rushing attacks.

VII. FUTURE CONTINUE

Based on the research that the author did, therefore, many things will need to be considered to develop this application to make it better in the future. The routing protocol used in this simulation can be replaced by proactive or hybrid routing protocols by using another type of malicious nodes and TCP protocol transmission.

It is expected that in the next research, a variety of scenarios will be evaluated through more complete QoS for more accurate parameters.

REFERENCES

[1] R. Sl, S. C. Desai, and R. Kt, "Performance Evaluation Of Aodv And Aomdv Routing Protocols In Wireless Mesh Network," 2013.

[2] J. Loo, J. Lloret Mauri, and J. H. Ortiz, *Mobile ad hoc networks : current status and future trends*. CRC Press, 2012.

[3] R. Ratnasih, R. M. N. Ajinegoro, D. Perdana, And D. Perdana, "Analisis Kinerja Protokol Routing AOMDV pada VANET dengan Serangan Rushing," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 6, no. 2, p. 232, Jun. 2018.

[4] N. P. Neetha Paulose, "Comparison of On-Demand Routing Protocols AODV with AOMDV," 2016.

[5] R. S. Lubis and M. Pinem, "Analisis Quality of Service (QoS) Jaringan Internet Di Smk Telkom Medan," 2014.

[6] A. Alamsyah, E. Setijadi, I. K. E. Purnama, and M. H. Purnomo, "Analisis Kinerja Protokol Routing Reaktif dan Proaktif pada MANET Menggunakan NS2," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 2, pp. 138–143, Jun. 2018.

[7] D. K. Lobiyal and V. Mansoura, *Next-Generation Networks*. Berlin: Springer, 2015.

[8] F. Uswatun Hasanah and N. Mubarakah, "Analisis Kinerja Routing Dinamis Dengan Teknik Rip (Routing Information Protocol) Pada Topologi Ring Dalam Jaringan Lan (Local Area Network) Menggunakan Cisco Packet Tracer," *Singuda ENSIKOM*, vol. 7, no. 3, pp. 118–124, May 2014.

[9] F. U. Hasanah and N. Mubarakah, "Analisis Kinerja Routing Dinamis dengan Teknik RIP (Routing Information Protocol) pada Topologi Ring dalam Jaringan LAN (Local Area Network) Menggunakan Cisco Packet Tracer," *Singuda Ensikom*, vol. 7, no. 3, pp. 118–124, 2014.