JURNAL INFOTEL
Informatics - Telecommunication - Electronics
Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Performance Analysis of Reactive Routing Protocol on VANET with Wormhole Attack Schemeaper

Ratnasih[1*], Doan Perdana[2], Triani Wulandari[3], M. Irfan Pratama[4]
[1,2,3,4]Telkom University
[1,2,3,4] Jl. Telekomunikasi No 1 Terusan Buah Batu 40257, Bandung, Indonesia
Corresponding email: ratnasih@outlook.com

Received 25 July 2018, Revised 02 August 2018, Accepted 06 August 2018

Abstract - Entering the information era, the current needs of the global community is increasing very rapidly. Vehicular Ad-hoc Networks (VANET) has drawn significant attention from both industry and academia as an important development of vehicular communication technology. VANET is one of open network and communication media without security mechanism. There are many kinds of security threat that can interrupt data communication in VANET. Wormhole attacks as one of security threat can be a good challenge in VANET security research. In this paper, we evaluate the performance of the reactive routing protocol on VANET with wormhole attack scheme. The project is simulated using NS-3 in Ubuntu platform with performance analysis of routing protocol by changing initial power and node density. We conclude that throughput values are increasing along with the changing of initial power while the delay values are decreasing rapidly. By the changing of node density, the highest delay value is 0.122 ns on 10 nodes condition and 0.215 Mbps for throughput value on 8 nodes condition.

Keywords – VANET, NS3, Wormhole Attack, Security, Threat.

I. INTRODUCTION

This Nowadays, information technology is developing rapidly in the global community. VANET is a network that used intelligence Transportation System to increase the safety and ease side while driving transportation [1]. VANET using Dedicated Short Range Communication (DSRC) with 5.9 GHz bands spectrum and bandwidth of 75 Mhz which has been allocated and with the range of climbing so that between a vehicle with a vehicle (V2V) and between vehicles and infrastructure (V2I) communicate with each other [2].

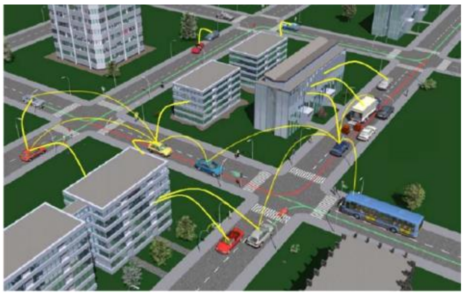

Fig.1. Vehicular Ad-Hoc Network [3]

In the Fig.1, It can be seen that between the car with the car performing communication direct communication through V2V, while cars with the infrastructure of the RSU uses communication V2I [3]. The wireless network is constantly evolving to meet the various needs of people, and vehicular communication isn't an exception. Vehicular Ad-hoc Networks (VANET) technology is a subclass of Mobile Ad-hoc Network (Manet). Comparing with Manet, VANET has high mobility and changing topology constantly in a short time [4]. The routing protocol that is frequently used on Network of Vehicular Ad-hoc Network (VANET) is a reactive routing protocol (On-demand). Reactive routing protocol search of the route in on-demand and set the link to send and receive packets from the source node to the destination node [5],[6].

Basically, VANET can be referred to as a relatively non-secure network, mainly because of the behavior of the broadcast on the wireless media in accordance with the needs of infrastructure architecture establishment. In addition, it has a decentralized architecture, and algorithm ad-hoc network relies on the participation of cooperative node on the network VANET [7]. This may be the opportunity of malicious nodes for an attack against the routing protocol. This attack is not only disturbing the search-routing process but can also interfere or cripple the performance of the routing protocol. A lot of security threat can interrupt data communication on VANET. Wormhole attacks are one security threat where two or more malicious nodes make a tunnel for transmitting the data to change the destination hop from that has been determined before [8]. Wormhole attack can be a good challenge in VANET security research. The main purpose of this project is to measure the impact of the wormhole attacks on reactive routing protocol in VANET using NS-3 software.

In the other paper [9], the writers examined VANET's challenges in rare network conditions, reviewed the using of epidemic routing and for partially connected VANET, they also proposed a Border node Based Routing (BBR) protocol. The simulation results that we get from the paper under rural network conditions, is that the limited flooding protocol such as BBR is performing well and offering the advantage of not relying on a location service required by other protocols that are proposed for VANET.

In 2013, in the paper "Security Threats on VANET: A Review Paper" [10], Ganesh, S.N., and Ranjani S. studied VANETs position which is becoming the platform of networking that would support the future vehicular communication service. They analyzed some of the security threats in VANET and the possible ways to overcome the problem and tell us that there is research which attempts to make VANET become real in the future. From this paper, various attacks and the remedies are presented. Next time they planned to develop the system to detect the main threat and verify it via simulation by imposing the new idea on the procedure for protecting the data.

In 2015, Raghuwanshi, V. and Jain, S. published a paper on "Denial of Service Attack in VANET: A Survey" [11]. In this paper, they have done a survey of attack on network availability and its severity levels in VANET environment, which known as Denial of Service (DOS) attack, along with that different kind of hybrid Denial of Service attack is also present in it with their existing solutions.

In 2012, Bibhu, V. Roshan, K. Singh, K.B. and Singh, D.K published a paper on "Performance Analysis of Black Hole Attack in VANET" [12]. They elaborated the various kinds of threat and their level in the ad-hoc network. The metric of performance is taken for the evaluation of threat which depends on the delay of the packet transmission, throughput and network load which is shown in Fig.2 until Fig.4. From this paper, we know that On-Demand Distance Vector Routing and Optimized Link State Routing make a lower level of the malicious node buffer size which can increase the drop of the packet.

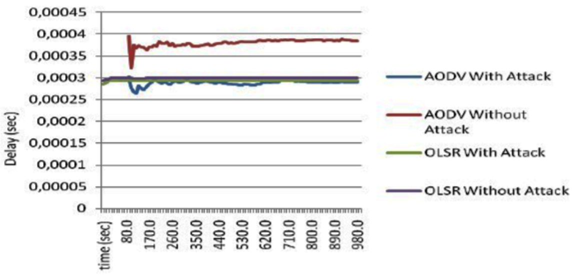

Fig.2. End-to-End Delay of OLSR and AODV With Vs. Without Attack For 16 Nodes [12]

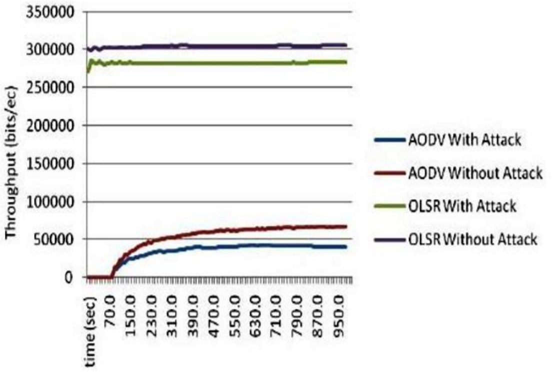

Fig.3. The Throughput of OLSR and AODV With Vs. Without Attack For 30 Nodes Attack [12]

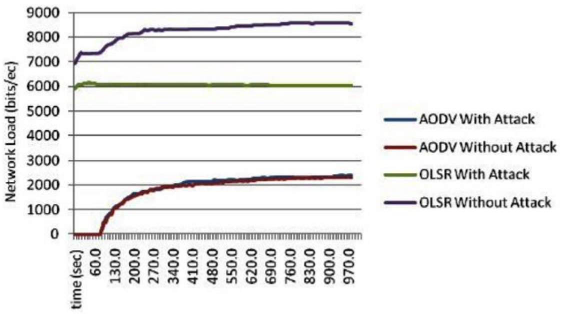

Fig. 4. Network Load of OLSR and AODV with vs. without attack for 16 nodes [12]

Based on the research above, we conclude that security is an important concern area for vehicular network application. VANET has the potential for improving the security and efficiency of future vehicular communication. In VANET, vehicles are considered to be intelligent mobile nodes which are able to communicate with their neighbors and the other vehicles in the available network [10].

II. RESEARCH METHOD

A. VANET

Vehicular ad hoc network (VANET) is a vehicle to vehicle (Inter-vehicle communication-IVC) and roadside to vehicle (RVC) communication system. The technology in VANET integrates WLAN/cellular and Ad Hoc networks to achieve the continuous connectivity. The ad hoc network is put forth with the novel objectives of providing safety and comfort-

https://doi.org/10.20895/infotel.v10i3.384

related services to vehicle users. Collision warning, traffic congestion alarm, lane-change warning, road blockade alarm (due to construction works etc.) are among the major safety related services addressed by VANET. In the other category of comfort related services, vehicle users are equipped with Internet and Multimedia connectivity [1]. Similar to mobile ad hoc networks (MANETs), nodes in VANETs self-organize and self-manage information in a distributed fashion without a centralized authority or a server dictating the communication. In this type of network, nodes engage themselves as servers and/or clients, thereby exchanging and sharing information like peers. Moreover, nodes are mobile, thus making data transmission less reliable and suboptimal. Apart from these characteristics, VANETs possess a few distinguishing characteristics, presenting itself as a particularly challenging class of MANETs is highly dynamic topology.

B. *Ad-hoc On-Demand Distance Vector (AODV)*

The reactive protocol used on this project, i.e. Ad-hoc On-Demand Distance Vector (AODV) Algorithm, also be referred to as a pure on-demand route acquisition system. In other words, nodes don’t depend on active path, keep routing information, or take a part in routing table exchange. A node doesn’t need to find and save a route until the node will communicate. Fig.5 is the example of AODV process.

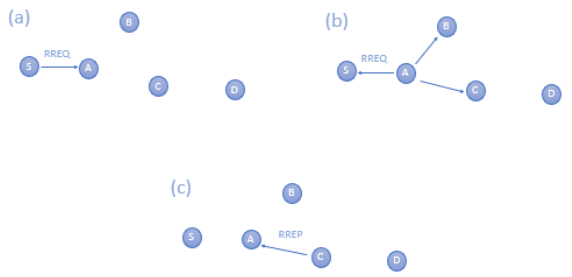

Fig.5. Route discovery process in AODV

We can see in Fig.5.(a) Node S will send message to Node D but Node S doesn’t have direct route to Node D. Then, Node S sent RREQ package to Node A. Node A makes an entry reverse route which heading to Node S with Node S as destination attribute, the next hop is Node S, and hop count value is 1. Because Node A doesn’t have a direct route to Node D, so it sent a broadcast package RREQ to other nodes (Fig.5.(b)). And then, Node C receives the RREQ package and makes entry reverse route with Node S as destination attributes, and the next hop is Node A, with hop count value is 2. Due to Node D is directly connected with Node C, so Node C has route information to reach Node D response the RREQ package with RREP (Fig.5.(c)). Node C makes RREP package which includes IP address attribute of Node D, a sequence number which is got from Node D response to Hello package which transmitted by Node C and hops count value to Node D is 1. This RREP package will be sent in unicast to Node A.

C. *Wormhole Attack*

Wormhole attack literally interpreted as an attack by the Attacker which resembles a wormhole to the path or route. Generally, Wormhole attack is a form of attack on a computer network (specifically using peer to peer topology), where a package of messages sent by the sender to the recipient's computer, changing the route by computer that acts as the attacker (Attacker), by making a link (line, tunnel, channel, route), which is like a wormhole.

This is caused by the absence of routing path verification and information regarding route by each computer which is involved. The main idea is to infiltrate into the network, copy the data packets which are being sent through a routing path, then make another path (tunnel or wormhole), and distribute the data package to a path that has been created, thus messing up the overall routing information. For more details, Fig. 6 is the illustration of wormhole attack process.

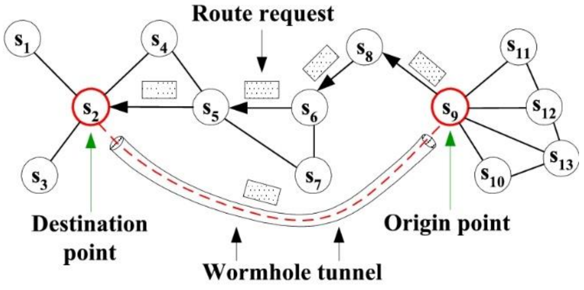

Fig. 6. Wormhole Attack Illustration [8]

From Fig.6, it can be seen that in this Wormhole Attack pattern, it was made a path or a tunnel as a new route or a way that will be traversed by data packet (either data information or message) from a sender computer to the computer of the recipient. The attack copies the package data, create a new path (the Tunnel), and then distribute copies of these data packages to the path that has been created. Note that the existence of the origin point and the destination point (the point of which has been determined by the attacker) and a path (Wormhole Tunnel) between them.

Other neighboring nodes or peer would have thought that the attacker is a node or a legitimate peer and be the source of the data packet, so that will affect whole routing information. The consequence will be very the fatal, where the data packets will never reach the destination or misused, because of going through the wrong or improper path. Imagine if the data package is important and secret [8].

D. *System Design*

The project starts with determining the VANET network topology. After that, we build the system configuration by installing NS3 environment in

Ubuntu system and patching the wormhole attack AODV routing. After the configuration is completed, we implement the scenario with the wormhole attack condition. The scenarios are the changing of initial power and node density. We collect the data of QoS and make an analysis from the data. The channel model in this research is ignored to be discussed.

E. Performance Test Parameter

Performance test parameter is one of the ways to find out the network performance and routing protocol performance. Performance test parameter is identical to the Quality of Service (QoS). In this project, we use the following QoS parameter [13][14].

a) Throughput

Throughput is the number of received packets on an interval of a particular observation time.

Formula for throughput:

Throughput = (rxBytes) / (obTime) (1)

In equation (1), rxBytes represents the total number of received bytes, obTime is the total of observation time

b) Delay

Delay is the amount of time which takes a packet data to travel from source to destination node.

Formula for delay:

Delay = (rxPackets) – (txPackets) (2)

In the equation (2), rxPackets represents the total time to packet arrive in the receiver, and txPackets is time to source send the packet.

c) Jitter

Jitter is the variance of the delay or the difference between the first delay with a further delay.

Formula for jitter:

Jitter= (jitterSum) / (rxPackets-1) (3)

In the equation (3), jitter sum represents the total variance of delay, and rxPackets-1 is the total packet that arrives in the receiver.

III. RESULT

Testing of simulation will be analyzed in NS-2.35 software. In this chapter, we do the analysis using a scenario. In this project, the parameter that will be analyzed is Throughput, Delay, and Jitter using Flow Monitor module [15]. Throughput is the number of received packets on an interval of a particular observation time. Delay is the amount of time which takes a packet data to travel from source to destination node. While jitter is the variance of the delay.

A. Performance Analysis of Routing Protocol by the Changing of Initial Power

This scenario uses the change of initial power as its parameters. The power in this scenario is referred to as transmission power in the amplifier. The initial power that was used starting from 35, 40 and 45 dB. Then the performance that we analyzed is throughput, delay, and jitter values.

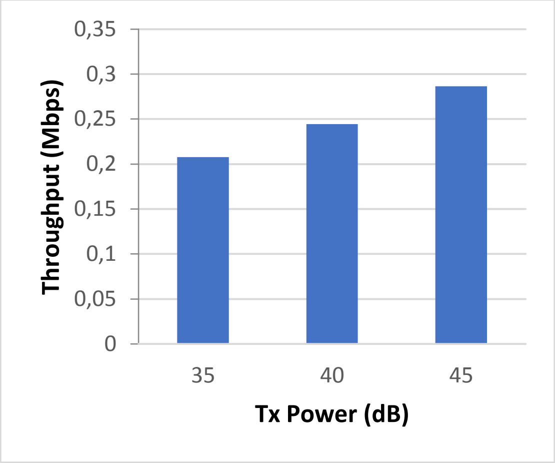

Fig7. Throughput Result of Changing Tx Power

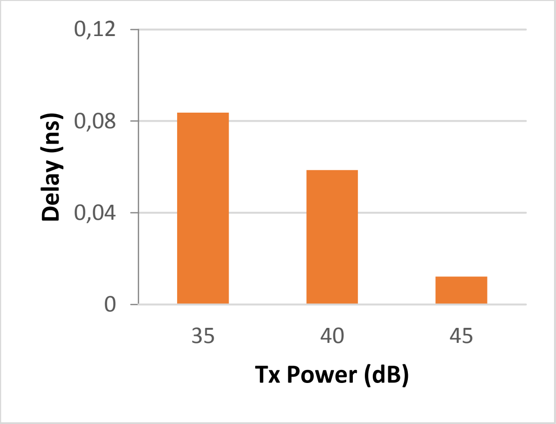

Fig.8. Delay Result of Changing Tx Power

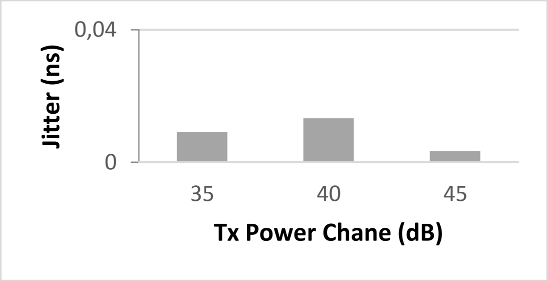

Fig.9. Jitter Result of Changing Tx Power

B. Performance Analysis of Routing Protocol by the Changing of Node Density-cased.

This scenario uses the change of node density as its parameters. The number of the node that used was starting from 6, 8, and 10. Then the performance that we analyzed is throughput, delay, and jitter values. It can be seen in Fig.10 until Fig.12 that VANET performance using reactive routing protocol against wormhole attack scheme by the changing of node density scenario with the value changes amounting to 6.8, and 10 nodes.

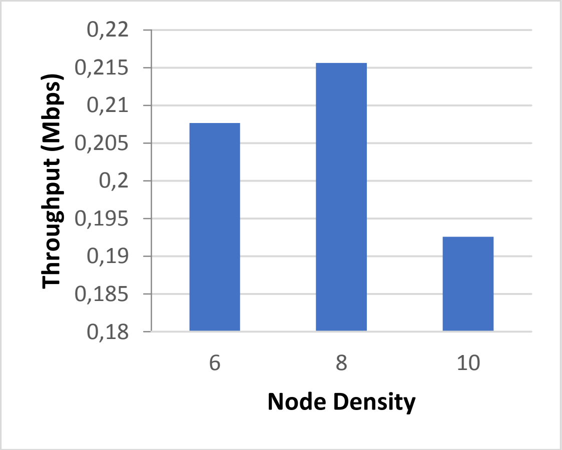

Fig.10. Throughput Result of Changing Node Density

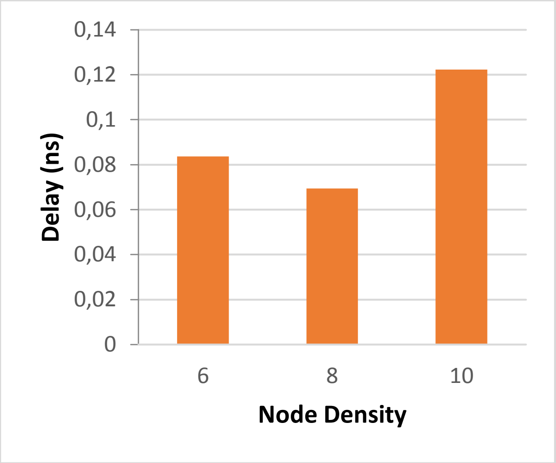

Fig.11. Delay Result of Changing Node Density

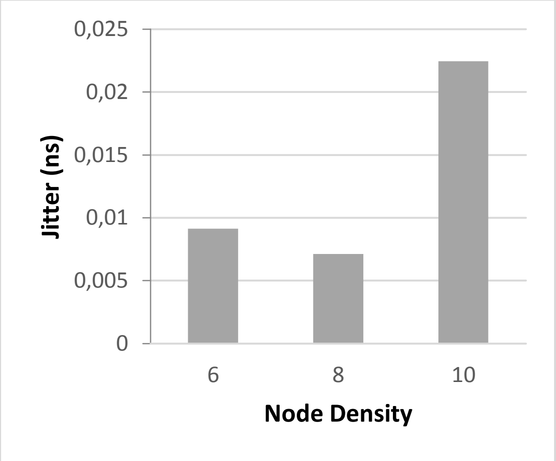

Fig.12. Jitter Result of Changing Node Density

IV. DISCUSSION

In order to calculate throughput, delay, jitter, we are used formula (1), (2), and (3). These parameters influence each other each other. From Fig. 7 it can be seen that value of throughput when VANET performance using reactive routing protocol against wormhole attack scheme by the changing of initial power scenario with the value changes amounting to 35, 40, and 45 dB resulting throughput getting bigger. With reference to the TIPHON (DTR/TIPHON-05001) standard, the throughput value is already in the excellent category ie> 100bps.

In contrast with the value of throughput, from Fig.8 it can be seen, the value of delay has declined when the tx packet is increased. But the value of delay still is in the excellent category by the TIPHON (DTR/TIPHON-05001) standard, ie <150ms.

From Fig.7 until Fig.9 it can be seen that value of throughput when VANET performance using reactive routing protocol against wormhole attack scheme by the changing of initial power scenario with the value changes amounting to 35, 40, and 45 dB resulting throughput goes up vertically where when the delay increases, delay experienced a considerable decline of 0.04 s. While the jitter value at the time the tx power 40 dB has the greatest value i.e. 0.013260925 s. It because when the power 40 dB, that have more interference as the formula (4) and (5).

As well as the result of tx packet changes, the result of changing the number of nodes also influences each other between parameters. On the node number change scenario, it produces fluctuating throughput delay and jitter. However, the highest value for jitter and delay is at the number of 10 nodes. So it will produce a small throughput value on the number of 10 nodes.

If a VANET communication using a point transmitter in absorption fewer media, its power is distributed to the outer area homogeneously of the sphere centered from the point transmitter. This sphere area is given by 4 π R^2, and the power per unit area is given by

$$Pt / (4 \pi R^2) \qquad (4)$$

Where Pt is the transmit power, A receiver with an aperture “A” will receive a power of,

$$Pr = Pt / (4 \pi R^2) \times A \qquad (5)$$

When we set a high initial power in constant distance condition, the amount of data received will increase so that the resulting throughput value will be greater and give the smaller delay value.

With Formula (4), (5), (1), and (2) we can conclude that when the power is getting smaller, then the delay will be increasingly enlarged and throughput will be progressively decreased. So that the data will be increasingly long to arrive at the receiver.

V. CONCLUSION

On the conditions with the absence of wormhole attacks, throughput performance by the changing of initial power scenarios: 35, 40, and 45 dB with considering the conditions that occur when sending data, ideally with sending 1024 bytes data packet, get average value of 1024 bytes because when sending data we consider that the data transmission uninterrupted.

On the conditions with the existence of wormhole attacks, throughput performance by the changing of initial power scenarios: 35, 40, and 45 dB with 1024 bytes data packet get the average value 0.1318305 bytes, this is due to the changing of hop that is already set in the initial state. It affects routing tables that already exist, so delivery mileage data on these scenarios becoming even further and resulting throughput values which are becoming smaller.

On the conditions of the existence of wormhole attacks, delay performance by the changing of initial power scenarios: 35, 40, and 45 dB gain delay value that are getting smaller when given an initial power that was growing while at the change of the node density, delay value is getting bigger because it is influenced by the number of the node itself, where the number of nodes increases but the initial power to be used remains the same.

REFERENCES

[1] N. K. Qureshi and A. H. Abdullah, "Topology Based Routing Protocols for VANET and Their Comparision with Manet," *Journal of Theoretical and Applied Information Technology,* vol. 58, no. 3, 2013.

[2] B. S. M., J. C. Bernandos and C. Guerrero, "Posisition Based Routing in Vehicular Netwroks : A Survery," *Journal of Network and Computer Application,* 2012.

[3] E. and A. , "Simulation of Vehicular Movement in VANET," *National Institute of Technology Rourkela,* 2013.

[4] K. "AODV Routing in VANET for Message Authentication Using ECDSA," in *IEEE Conference on Communication and Signal Processing (ICCSP),* 2014.

[5] S. Sulistyo and S. Alam, "Distributed Channel and Power Level Selection in VANET Based on SINR using Game Model," *International Journal of Communication Networks and Information Security (IJCNIS),* vol. 9, no. 3, pp. 432 - 438, 2017.

[6] R. A. and M. K. Mishra, "Mobility Adaptive Density Connected Clustering Approach," *International Journal of Communication Networks and Information Security (IJCNIS),* vol. 9, no. 2, pp. 222 - 229, 2017.

[7] E. Mustikawati, D. Perdana and R. M. Negara, "Network Security Analysis in VANET Against Black Hole and Jellyfish Attach with Intrusion Detection Algorithm," *CommIT (Communication & Information Technology,* vol. 11, no. 2, pp. 77 - 83, 2017.

[8] I. P. E and P. Sukanto, "Wireless Sensor Network Teori & Praktek Berbasiskan Open Source," 2015.

[9] M. Zhang and R. S. Wolff, "Routing Protocols for Vehicular Ad Hoc Network in Rural Areas," pp. 1-8.

[10] S. G. N., "Security Threats on Vehicular Ad Hoc Networks (VANET) : A Review Paper," vol. 4, no. 6, pp. 196 - 200, 2013.

[11] R. V. and S. Jain, "Denial of Service Attack in VANET : A Survey," vol. 28, no. 1, pp. 15 - 20, 2015.

[12] V. Bibhu, "Performance Analysis of Black Hole Attack in VANET," pp. 47 - 54, 2012.

[13] T. Wulandari, D. Perdana, and R. M. Negara, "Node Density Performance Analysis on IEEE 802.11ah Standard for VoIP Service," *International Journal of Communication Network and Information Security (IJCNIS),* vol. 10, no. 1, 2017.

[14] D. Perdana and R. F. Sari, "Performance Evaluation of Corrupted Signal Caused by Random Way Point and Gauss Markov Mobility Model on IEEE 1609.4 Standards," *Next Generation Electronics (ISNE),* 2015.

[15] G. Carneiro and M. Ricardo, "FlowMonitor - a network monitoring framework for the Network Simulator 3 (NS-3)," [Online]. Available: telecom.inestec.pt/~gjc/flowmon-presentation.pdf. [Accessed 29 March 2017].