

# Network Security Analysis in Vanet Against Black Hole and Jellyfish Attack with Intrusion Detection System Algorithm

Elsa Mustikawati<sup>1</sup>, Doan Perdana<sup>2</sup>, and Ridha Muldina Negara<sup>3</sup>

Faculty of Electrical Engineering, Telkom University, Bandung 40257, Indonesia

Email: <sup>1</sup>elsamustikawati@gmail.com, <sup>2</sup>elsamustikawati@gmail.com ,

<sup>3</sup>ridhanegara@telkomuniversity.ac.id

**Abstract**—VANET is the key to the Intelligent Transportation Systems (ITS), where vehicles can communicate with others to exchange information in real time. VANET is an ad-hoc that has no fixed infrastructure and rapidly changing network topology. As the result, the network is insecure and vulnerable to various attacks both from within and outside the network. This research analyzes AODV routing protocol comparing the conditions without the attacks and with the attacks with the of black hole and jellyfish using the algorithm of Intrusion Detection System with the number of nodes changing from 10 to 100 nodes at the change speeds of 70, 80, 90, 100, 110, and 120 km/h. This research is simulated using Network Simulator 2 to model the network and ONE Simulator to model node mobility. The analyzed QoS parameters are packet delivery ratio (PDR), throughput, and end-to-end delay. The results of the simulation show that changing the number of nodes and node velocity affects the performance in the network. On the number of nodes scenario with attacks, the average value of PDR decreases by 48.03%, throughput decreases by 50.23%, and delay, for black hole, decreases by 80.18% but increases by 47.87% for jellyfish. Whereas in the node velocity scenario, the average values of PDR, throughput, and delay decrease by 58.52%, 60.34%, 13.81% for black hole attack, respectively. However, the delay increases by 123.91% for jellyfish attack.

**Index Terms**—Black hole attack, IDS, jellyfish attack, and VANET

## I. INTRODUCTION

VEHICULAR Ad Hoc Network (VANET) is an ad-hoc network that allows vehicles to communicate with others without any fixed infrastructure. VANETS is a promising approach to intelligent transportation system (ITS) [1]. A network system that connects to the Internet requires better protection in usage because it has a high threat level [2]. Ad-hoc network has a decentralized architecture and algorithm in ad-hoc

network relies on the participation of cooperative node on the network VANET. So any decision making is decentralized, it can be used by attackers to perform the attack. The attack aimed to destabilize a running cooperative algorithm [3]. It makes VANET network vulnerable to attacks that can cause problems even on small networks. In addition, it can pose a threat to network security that can worsen the function or network services. Among all the existing challenges, network security on VANET less noted for this. Data packets in VANET contains information critical and needs to be ensured that those packages are not accessed or modified by attackers. Network security issue is not similar to the communication network in general. The size of the network, mobility, geographic relevance, and other things to make this implementation difficult and different from other network security [4].

Reference [5] studied that black hole attack reduces packet delivery fraction to 10%–40%, but when there are the addition algorithm IDS, up to 90%–98%. The algorithm IDS have the advantage of not requiring the addition of overhead and slight modification of AODV. Reference [6] simulates jellyfish attack using AODV routing protocol on a network of MANET. The results of these simulations that the jellyfish affects network performance with improving end-to-end delay and jitter. Based on previous related research, can be drawn the conclusion that the offensive black hole and jelly fish can be solved by doing a modification on the routing protocols that are used namely AODV. Because some attacks carried out modifications to the RREP message that interferes with the process of routing. So counterfeited RREP message, which seems malicious nodes have the latest and fastest routing.

In this research, to prevent the attacks, IDSAODV is used as prevention algorithm for both attacks in two scenarios. The vehicular environment is modeled

in highway road, which took Jakarta-Cikampek Toll Road.

This article is decomposed into five sections. Section II presents the basic theory in this research. Section III presents the model used in the current research. Section IV discussed the simulation result and analysis according to the data and theory. Finally, Section V briefly restates the research problem and summarizes the current finding

## II. THEORY

### A. Vehicular Ad-Hoc Network

VANET is wireless ad-hoc that allows communication between vehicles or vehicles with devices on the roadside. With purpose, that enhances the security of transportation. The movement of the vehicles or node on VANET is very dynamic because the vehicle moving at a high speed and the position changes constantly. These characteristics make network topology change rapidly, so the link between node connect and disconnect very often [7].

The communication mode on VANET can be classified into two categories. Vehicle-to-vehicle (V2V) communications mode is mode communication between the nodes on the vehicle or On-Board Unit (OBU). Vehicle-to-infrastructure (V2I) road is a mode of communication between nodes or vehicles with hardware on the roadside or Road Side Unit (RSU) [7].

### B. Ad-Hoc on Demand Distance Vector

Ad-hoc On Demand Distance Vector (AODV) routing protocol is the reactive and on-demand routing protocol. The routing table will only update when the source and destination nodes need to transmit data packets. AODV routing protocol operates in two stages, namely, route discovery and route maintenance [5]. When the source node wants to communicate with the destination node, but do not have the route, then the source node will initialize the route discovery process. AODV route discovery process uses control messages to determine the route to the destination node. There are three control messages of route discovery as below:

1) *Route Request*: Route Request (RREQ) will be sent when the source node wants to send a packet to the node that is not a node’s neighbors and who have not establish the route. Source node will broadcast the RREQ to all nodes, which is adjacent to the source node. In Table I presents fields in RREQ message. In the RREQ message, there is a hop count field that states the number of hops that must transmit by the RREQ. In addition, there is broadcast ID and a sequence number that serves to avoid the sending of the same message to a node.

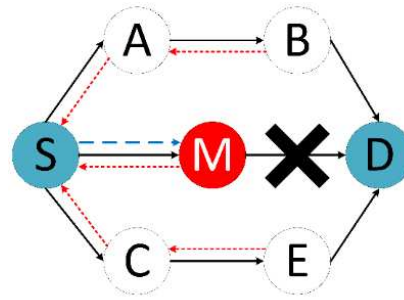


Fig. 1. Black hole attack mechanism.

2) *Route Reply*: When the nodes receive Route Reply (RREP) packets, the nodes will look up to its routing table whether it has a route to the destination or not. If the node has a route to the destination or the destination itself, it will send the RREP packets. When the RREP packet arrived on the source node, then the route will be established through the intermediate nodes and path, assuming that it is the fastest route [8]. Table II is the fields inside RREP message.

### C. Black Hole Attack

Black hole node sends false routing information, claiming that the node has the fastest route. By manipulates the RREP field, using highest sequence number and hop count was set to 1, causing the intermediate nodes send data packets to malicious nodes. After the route is established to black hole node, it will drop all the packets without forwarding the packet to the other nodes [9].

### D. Jellyfish Attack

Jellyfish attack can be classified into three subcategories; jellyfish delay variance attack is applied in this research. First, jellyfish node will manipulate the other nodes to establish the route to itself by using false RREP. In this research, it was applied by changing highest sequence number field and hop count was set to 1. After the route is established, jellyfish node adds a delay on each packet before forwarding the packet, without changing the sequence of the packet. Delay can vary from 0 to 10 s randomly [6]. In this research, delay varies from 0 to 2 s randomly before forwarding the packet.

### E. Intrusion Detection System

Intrusion Detection System (IDS) is a system for detecting intrusion or interference on the network by collecting, analyzing and auditing system of the data

TABLE I  
RREQ MESSAGE FIELD [8].

Source_address	Source_sequence	Broadcast_id	Destination_address	Destination_sequence	Hop_count
----------------	-----------------	--------------	---------------------	----------------------	-----------

TABLE II  
RREQ MESSAGE FIELD [8].

Source_address	Destination_address	Destination_sequence	Hop_count	Lifetime
----------------	---------------------	----------------------	-----------	----------

on the network. IDS monitor activities continuously, as for example traffic package is passed.

IDSAODV assumes that the RREP message first to come is RREP message from malicious nodes. In route discovery process, the first RREP message arrived is ignored and the second RREP arrives is chosen to establish the routing path. This mechanism is called RREP caching mechanism. In Network Simulator 2, four functions are added into `idsaodv.cc`, which is `rrep_insert` to add the RREP message, `rrep_lookup` to check whether there is another RREP message, `rrep_remove` to remove all the records from the other until the RREP message from a particular node and `rrep_purge` to remove the RREP periodically if it has expired. IDSAODV will choose the second RREP arrived as the routing path, whether it comes from malicious node again or not [10].

### III. RESEARCH METHOD

To prevent black hole and jellyfish attack, IDSAODV is applying to prevent or reduce the effects of network performance. Inside IDSAODV, there are RREP caching mechanism to reduce the effects of the attack by ignoring the first RREP packet. Figure 2 shows RREP caching mechanism in IDSAODV. First, the node will wait for the first arrived RREP packet. If the first RREP packet arrived, IDSAODV will ignore it and wait for the next RREP packet. The node will establish routing patch through the node that sends the next RREP packet.

This RREP caching mechanism assumes that the first RREP packet comes from the black hole or jellyfish node which contains false RREP. In the black hole and jellyfish attack, the malicious node will send false RREP that contains the highest sequence number and hop count was set to one that will manipulate the other nodes to establish routing patch to itself. With IDSAODV, the first RREP packet is ignored and it will reduce chances to establish the routing path to the malicious node.

Mobility route in this research took Jakarta–Cikampek toll road from KM 47–54. The parameter of this simulation can be seen in Table III.

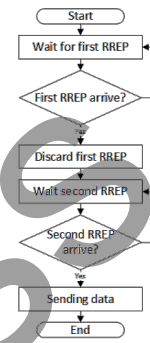


Fig. 2. Flowchart of RREP caching mechanism in IDSAODV.

TABLE III  
SIMULATION PARAMETERS

Parameter	Detail
Simulation Dimension	8000 × 1000
Simulasi Duration	400 seconds
Node Density	10 to 100 nodes
Node Velocity	70, 80, 90, 100, 110, 120 km/h
Routing Protocol	AODV, idsAODV
Malicious Node	Single Blackhole or Single Jellyfish
Mobility Model	Map Based Movement
Traffic Direction	Two ways
MAC	MAC 802.11 Ext (IEEE 802.11p)
PHY	Wireless 802.11 Ext (IEEE 802.11p)
Propagation Wave Model	Two Ray Ground
Antenna Type	Omnidirectional
Transport Layer	UDP
Traffic Model	CBR

This simulation consist of two scenarios, node density that varies from 10 to 100 nodes and node velocity that varies from 70 to 120 km/h. The number of nodes was generated by modifying number nodes configuration of .tcl file inside Network Simulator 2. Each node models a vehicle. For the node velocity scenario, the vehicle speed is modeled using ONE Simulator by setting the minimum and maximum speed of each node. Each node is moving based on the mobility route. Each simulation scenario for each configuration consist of five conditions, normal, under black hole attack, under black hole attack with IDS, under jelly fish attack and under jellyfish attack with IDS.

Traffic is modeled as constant bit rate with UDP as transport layer protocol. Total average packet sent was

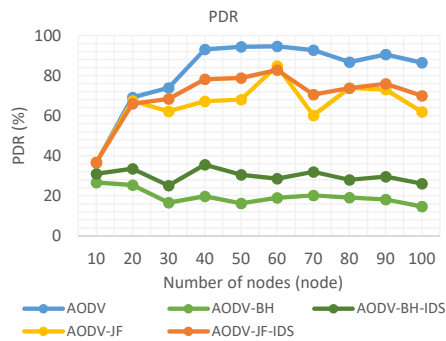


Fig. 3. Packet delivery ratio graph for node density scenario.

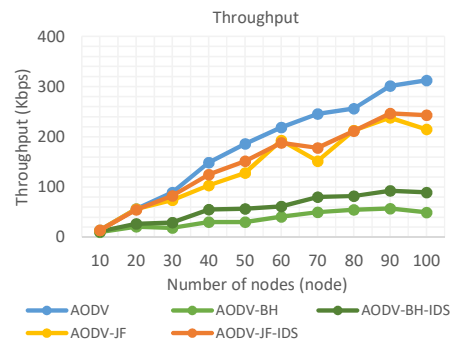


Fig. 4. Throughput graph for node density scenario.

31011 and total packet received was 29150 for normal condition based on 30 times generated traffic.

#### IV. SIMULATION RESULTS AND ANALYSIS

##### A. Node Density Scenario

In this scenario, the changes to the number of nodes that are used, i.e., 10, 20, . . . , 100 nodes at 70 km/h.

These scenarios were simulated in normal condition, under black hole and jellyfish attack and the addition of IDS algorithm.

In Fig. 3 shows that the PDR value has some fluctuations but it tends to decrease. Increasing number of nodes causing changes of network topology. Therefore, the routing path is changing for every amount of nodes. AODV shows the graph for normal condition, AODV-BH shows the graph for black attack condition, AODV-BH-IDS shows the graph for black hole attack condition with IDS, AODV-JF shows the graph for jelly fish attack and AODV-JF-IDS shows the graph for jelly fish attack with IDS.

Meanwhile, the average value of PDR under black hole attack decrease by 76.13% from the normal condition and under jellyfish attack decrease by 19.94% from the normal condition. The black hole attack dropping the entire packet in the network, while jellyfish attack still forwarding the packet. Graph of the PDR value under jellyfish attack always greater than black hole attack, because IDS algorithm will ignore the first RREP packet and use the second RREP packet arrived to establish the route. For black hole attack with IDS, the PDR value increase by 53.34% and for jellyfish attack with IDS increase by 6.99%.

In Fig. 4 shows that the throughput value increase along with changes the number of nodes in all conditions. This is due to increase of the number of nodes, the more packets that are sent and received, the traffic in the network keeps increasing. Increasing the number of nodes also takes the process of route discovery longer than AODV condition. Each node

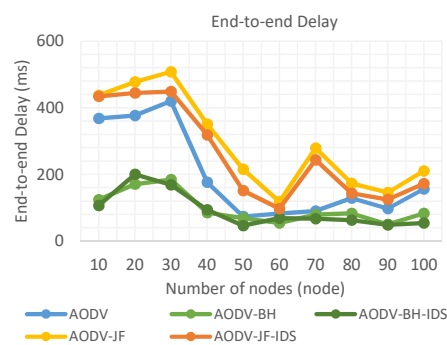


Fig. 5. End-to-end delay graph for node density scenario.

will look for the best routing with sends an RREQ message to its neighbor nodes and the destination nodes will send RREP message in return and unicast. Therefore, the more the number of nodes in the network, then the greater the throughput values on the network. Black hole and jellyfish attack decrease the throughput value in the network. Under black hole attack, the average throughput value decreased drastically by 80.18% or 146.66 Kbps from the normal condition. While under jellyfish attack, the throughput value decreased by 24.28% or 44.42 Kbps from the normal condition. In other words, black hole attack affects more on throughput parameters compared to jellyfish attack. This is because, the black hole node sends a false RREP message in reply to RREQ sender node, aiming to manipulate the routing path so that the malicious node seems to have the latest routing updates by replacing the sequence number into highest sequence number or 4294967295 and the nearest route by replacing the hop count to 1. That way, the process of route discovery took faster than normal condition. In other words, exchange routing message is less than the normal condition and the throughput decreased.

In Fig. 5 shows that the average end-to-end delay value changes in the addition number of nodes. The end-to-end delay value has some fluctuations but it

tends to decrease along with addition number of nodes. This fluctuation due to several factors, namely, traffic data, network topology, and the position of each node. Those things result in fluctuations of the simulations due to routing path that varies each amount of nodes. Under black hole attack, the average delay is decreased by 50.12% or 98.76 ms compared to normal conditions. This is due to under black hole attack, route discovery process lasts faster than normal condition. So that the nodes do not need to wait for RREP because the nearest black hole would immediately send a false RREP message. The purpose of it to manipulate the other nodes to establish the routing path to a malicious node, and dropping all the packets. Therefore, the route discovery process becomes shorter than normal condition. Whereas the normal condition carried out the process of discovery route in accordance with the mechanism of AODV routing protocol. In other words, the nodes will continue to do the broadcast RREQ to get reply message with the nearest routing RREP, which indicates that the node's neighbors destination node. Therefore, the average value of end-to-end delay on conditions without any attack greater than the conditions in the black hole [11, 12].

Jellyfish attack highly affects the value of end-to-end delay on the network. The value of end-to-end delay under jelly fish attack is 47.87% greater compared to normal conditions. This is due to this type of attack, which is jellyfish delay variance attack. Where the malicious node will forward the data package after delaying few seconds randomly on each packet within 0 to 2 seconds in this research. The value of end-to-end delay under jellyfish attack is higher than other conditions. In other words, jellyfish attack affects more than black hole attack.

The addition of IDS algorithm can reduce end-to-end delay in the offensive black hole and jellyfish attack. Under black hole attack, the average value of end-to-end delay is likely to decrease by 16.67%, although a number of nodes value is greater than under black hole attack. While the jellyfish attack, the average value of end-to-end delay is decreased by 11.50% compared to under jellyfish attack. The decrease in the value of end-to-end delay is due to both attacks sends the false RREP message that aims to take over routing patch to the malicious node itself. So the data packets will be sent to the malicious node and the attack took place. With added the IDS algorithm, then the malicious node will perform additional RREP caching mechanism to the routing process to avoid malicious nodes in the network, so the data packets are not forwarding through or stop at the malicious node.

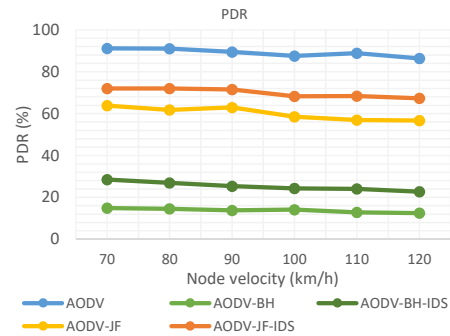


Fig. 6. Packet delivery ratio graph for node velocity scenario.

### B. Node Velocity Scenario

In this second scenario, the analysis is carried out based on the change of velocity of the node in several conditions. As for the change of velocity varies from 70, 80, 90, 100, 110, and 120 km/h. With the same number of nodes, i.e., 100 nodes in all conditions and parameters. While the performance parameters based on QoS parameters, which is Packet Delivery Ratio, and Throughput and End-to-end delay.

In Fig. 6 shows that the value of PDR from all condition has decreased along with the addition of node velocity. Normal conditions have the highest PDR value compared to the other conditions. However, the value of PDR on normal conditions has decreased slightly along with the addition of node velocity. This is due to the faster moving nodes in the network then the possibility of termination of communication links between nodes is getting bigger, so the value of PDR decreasing.

In addition, the average PDR value under black hole attack decrease by 84.53% from the normal condition. While in jellyfish attack, the PDR value decrease by 32.5% from normal conditions. With the node velocity scenario, then the termination of node link communication is faster and often occurs so that the packages have not had transmitted the data packets but the link has been disconnected beforehand.

On the conditions of the addition algorithm IDS as a response to the attacks of black hole and jellyfish. For the black hole attack with the addition of IDS algorithm, the average PDR value of PDR increases by 83.69% from under black hole attack condition. For jellyfish attack with IDS. The PDR value increase by 16.3% from under attack. The increase in PDR value is due to the RREP caching mechanism in IDS, first RREP message ignored and passed through the next RREP message arrived.

In Fig. 7 shows the throughput value of all conditions tends to decrease along with the addition of node



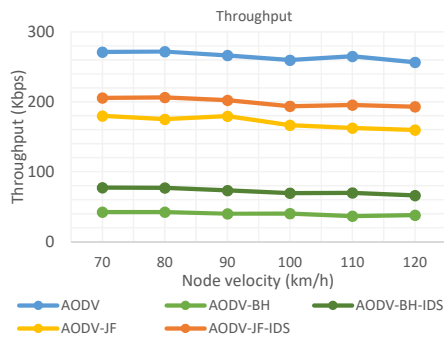


Fig. 7. Throughput graph for node velocity scenario.

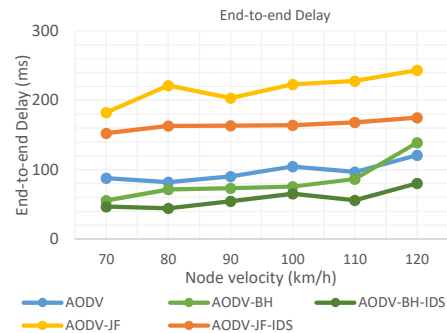


Fig. 8. End-to-end delay graph for the second scenario.

velocity. This happens due to the increasing speed of movement of a node, the termination of the communication link will be more frequent and the process of route discovery becomes disturbed. It can cause a decrease in the throughput value of the network. Black hole attack decreases the throughput value by 84.98% from normal conditions. While in jellyfish attack, the throughput value decrease by 35.71%. In other words, the black hole attack affects more than jellyfish attack. This is because the black hole attack did dropping packet, while in jellyfish attack still forwarding the packet.

On the addition of IDS algorithm, can be seen that the throughput value increase by 80.79% of from normal condition. While in jellyfish attack, the throughput value increase by 16.97% from the normal condition. With the addition of IDS algorithm results in increasing the throughput value for both attack. Because the algorithm IDS will ignore the first RREP message assuming that it comes from the malicious node and uses the next RREP message arrived as a routing path.

In Fig. 8 shows that the end-to-end delay graph for all conditions. Overall, the average value of end-to-end delay in all conditions of has decreased along with the increase of velocity. This is because with increasing speed of nodes, then the greater the possibility of disconnection of communication links between nodes. Under normal conditions, it would result in nodes has to be looking for the latest continuous routing due to network topology change rapidly. Therefore, end-to-end delay value keeps increasing along with the addition of node velocity.

Under black hole attack, the end-to-end delay value has some fluctuations. At speed of 90 km/h, the end-to-end delay value increases, but at speed of 100 km/h and 110 km/h it decreases. Overall, the end-to-end delay value is decreased by 13.81% from normal condition, but at speed of 120 km/h, it increases by 14.85% from normal conditions. The black hole node performs the modification process that causes the RREP route

discovery to take place faster so that the value of end-to-end delay is much smaller than the normal condition. As the node speed increase of the speed, the communication link termination occurs more frequent, so that at a speed of 120 km/h, the value of end-to-end delay is higher than normal conditions.

Under jellyfish attack, the end-to-end delay value increases by 123.19% from the normal condition and has some fluctuations at speed of 80 km/h and 90 km/h, but tends to increase along with the increasing speed of the node. This is due to jellyfish node wait 0 to 2 s before forwarding packet to other nodes, so the end-to-end delay value will be higher than normal condition.

On the conditions of the addition algorithm IDS addition, the value of end-to-end delay has decreased for both attacks. The addition algorithm IDS on black hole attack can decrease the end-to-end delay value by 30.69% from black hole condition. Although the value of end-to-end delay on the addition algorithm still has fluctuations along with the addition of the node speed but tends to increase along with the increasing speed of node. For the jellyfish attack and IDS algorithm, the end-to-end delay value decrease by 24.18% from under attack. This happens because in the addition of the IDS there is an RREP caching mechanism that assuming the first RREP packet arrive comes from malicious nodes. So that the routing path will establish using the next RREP packet arrives.

## V. CONCLUSION

The addition of IDS algorithm can increase the performance of the network based on the QoS parameters, namely the PDR, throughput, and end-to-end delay compared with conditions under attack. The average values of PDR on the black hole attack increase by 53.34% in Scenario 1 and 83.69% in Scenario 2. For jellyfish attack, the average values of PDR increase of 6.99% in Scenario 1 and 16.3% in Scenario 2. The average value of throughput on black hole attack increase

by 61.24% or 22.20 kbps on Scenario 1 and 80.79% or 3.1833 kbps on Scenario 2. For jellyfish attack, average throughput increase by 7.96% or 11.02 kbps on scenario 1 and 16.97% or 28.92 kbps on scenario-2. The average value of end-to-end delay under black hole attack decrease by 6.53% or 6.41 ms on Scenario 1 and 30.69% or 25.69 ms in the 2nd scenario. For jellyfish attack, the average value of end-to-end delay is decreased by 11.5% or 33.51 ms on Scenario 1 and 24.18% or 52.40 kbps for Scenario 2.

#### REFERENCES

- [1] A. Muhtadi, D. Perdana, and R. Munadi, "Performance evaluation of aodv, dsdv, and zrp using vehicular traffic load balancing scheme on vanets," *International Journal of Simulation System, Science and Technology (IJSSST)*, pp. 13.1–13.7, 2015.
- [2] B. Heru, B. Benny, D. Defendy, and W. Hento, "Keamanan jaringan menggunakan unified threat management pada server berbasis linux," *CommIT (Communication and Information Technology) Journal*, vol. 1, no. 1, pp. 48–59, 2007.
- [3] D. Perdana, M. Nanda, R. Ode, and R. F. Sari, "Performance evaluation of puma routing protocol for manhattan mobility model on vehicular ad-hoc network," in *Telecommunications (ICT), 2015 22nd International Conference*. IEEE, 2015, pp. 80–84.
- [4] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 5, no. 5, 2013.
- [5] K. S. Nisha and S. K. Arora, "Analysis of black hole effect and prevention through ids in manet," *American Journal of Engineering Research (AJER)*, vol. 2, no. 10, pp. 214–220, 2013.
- [6] H. R. Khirasariya, "Simulation study of jellyfish attack in manet using aodv routing protocol," *Journal of Information, Knowledge, and Research in Computer Engineering*, vol. 2, no. 2, pp. 344–347, 2013.
- [7] L. Wenshuang, L. Zhuorong, Z. Hongyang, W. Shenling, and B. Rongfang, "Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, pp. 1–11, Jan. 2015.
- [8] L. Mamta and P. Sharda Prasad, "Simulation of blackhole attack," *International Journal of Engineering Technology & Management Research (IJETMR)*, vol. 2, no. 2, pp. 23–30, 2014.
- [9] A. K. Gupta, N. Kaur, and A. Kaur, "A survey on behaviour of aodv and olsr routing protocol of manets under black hole attack," *International Journal of Computer Science & Technology*, vol. 2, no. 4, pp. 349–352, 2011.
- [10] S. Dokurer, "Simulation of black hole attack in wireless ad-hoc network," Master's thesis, Ankara, Atilim University, 2006.
- [11] V. Bibhu, R. Kumar, B. S. Kumar, and D. K. Singh, "Performance analysis of black hole attack in vanet," *International Journal Of Computer Network and Information Security*, vol. 4, no. 11, pp. 47–54, 2012.
- [12] B. Cherkaoui, A. Beni-hssane, and M. Erritali, "A clustering algorithm for detecting and handling black hole attack in vehicular ad hoc networks," in *Advances in Intelligent Systems and Computing*. Springer, 2017, pp. 481–490.