ISSN 2355-3286

Black Hole Detection Using Modified Sequence Number in Vehicular Ad-hoc Network

Rakha Fikran Julda[1], Dany Primanita Kartikasari[2], Rakhmadhany Primananda[3]
[1,2,3] Informatics Engineering, Brawijaya University, Malang, Indonesia
[1]rakhafikran@gmail.com, [2]dany.jalin@ub.ac.id, [3]rakhmadhany@ub.ac.id

Accepted 08 September 2022
Approved 20 October 2022

Abstract*— Vehicular Ad-hoc Network (VANET) is a type of wireless network with Dedicated Short-Range Communication (DSRC) that enables communication between vehicles (V2V) and communication between vehicles to infrastructure around them (V2I). VANET has several security requirements to consider in order to maintain the network functionality. Availability is the most important security requirement due to its responsibility of maintaining the functionality of the network, attack on availability may cause the lack of availability and reduce the efficiency of VANET. One of the attack that threat the availability of VANET is black hole. In this paper, we address the problem of black hole attack in VANET, using Modified Sequence Number (MSN) as a detection method. The simulation is performed using NS-2 as a simulator and AODV as a routing protocol. Detection Rate (DR) and False Alarm Rate (FAR) are used to evaluate the performance of MSN algorithm in detecting black hole attack. Evaluation with variation in the number of CBR packets shows that MSN algorithm successfully detects black hole attacks with DR values reaching 69.0909% at 10 CBR packets and FAR values reaching 0.0037 at 20 CBR packets. We also evaluate the performance of MSN algorithm with variations of node density. The evaluation shows that MSN algorithm successfully detects black hole attack with DR values reaching 100% with a density of 10 and 20 nodes, with the percentage of FAR values reaching 0% in all numbers of node density.

***Index Terms*— AODV; Black Hole Attacks; VANET**

I. Introduction

VANET is a dedicated short-range communication (DSRC) wireless network technology that works on the 5.9 GHz frequency spectrum for communication between vehicles. Unlike MANET which uses IEEE 802.11a/g/n, the physical layer of VANET uses the IEEE 802.11p standard protocol with its focus on communication in Intelligent Transportation Systems (ITS) environment [1]. In VANET, there are two types of communication that take place. Vehicle-to-Vehicle (V2V) is a communication between vehicles, whereas Vehicle-to-Infrastructure (V2I) communication is between vehicles and infrastructure such as Roadside Units. (RSU) [2]. VANET has several parameter to ensure its network security, including integrity, authentication, availability, privacy, and non-repudiation. Attackers exploit these security parameter to carry out their attack. The primary role of availability to guarantee the network services continue to work in the event of malicious attacks is what makes availability one of the most important parameter in VANET security, as its lack of availability may diminish the efficiency of VANET [3]. One of the attack that threat the availability of VANET is black hole [4]. Black hole use the routing protocol's route discovery process which searches for the nearest route, by pretending to be the node with the newest and shortest path to destination. The black hole node that receives the packet drops the packet so that the packet is not received by the destination. The routing table of the routing protocol is disrupted by the behavior of black hole attacks, reducing the performance efficiency of VANET [5]. Therefore, a routing protocol that can works on network with dynamic topologies, high mobility, and able to protect against attacks such as black hole is required.

In attempt to secure VANET from black hole attack, several research has been done. Among these is using a protocol called Secure AODV (SAODV). The proposed routing protocol changes the destination IP address of AODV packet request by applying Cyclic Redundancy Check 32 bits (CRC-32) as a hash function, resulting a secure AODV RREQ packet without any extra overhead. The test results in this study explain that the proposed protocol successfully addresses black hole attack with PDR performance, end-to-end delay, routing overhead, and throughput that is nearly identical to traditional AODV. Additionally, the proposed protocol has a high detection rate at both high and low node density [6]. However, the research has not shown the performance of SAODV in dealing with black hole attack with variation in number of packets sent. The variation in number of packets sent can determine how well a method to detect black hole attack [7]. Therefore, we use a scenario with different number of Constant Bit Rate (CBR) packet sent to measure the performance of our propose method.

Another research to secure wireless network from black hole attack is by implementing Modified Sequence Number (MSN) in MANET by using Route Reply (RREP) Sequence Number (SN) as the threshold. The threshold is set based on the highest SN value that the source can accept. When the source receive an RREP packet with a SN value above the threshold, the source will rebroadcast RREQ packet using RREP SN as the source SN. When the source receives a RREP message from the same node and the SN value of the RREP still exceeds the specified threshold, it will detect the route with the black hole node and is not used to forward the data. The research shows that the proposed method has higher PDR and throughput values in dealing with black hole at both low and high node densities compare to normal AODV and IDS [8]. The research, however, has not shown how well MSN in detecting black hole attack in AODV. Therefore, we use detection rate as a parameter to evaluate our propose method in detecting black hole attack.

According to prior research that assessed the performance of AODV on VANET, the fall in packet delivery ratio (PDR) on the performance of AODV in black hole attack reached 60% [6]. Therefore, a method that capable of protecting VANET from black hole attack is needed. In this paper, we propose a method to detect black hole attack in VANET by implementing MSN with AODV routing protocol. The performance of MSN algorithm in detecting black hole attack is tested based on variations in the number of Constant Bit Rate (CBR) packets and node density using Network Simulator 2 (NS-2).

II. Literature Review

A. Vehicular Ad-hoc Network

Vehicular Ad-hoc Network (VANET) Vehicular Ad Hoc Network (VANET) is a development of Mobile Ad Hoc Network (MANET) technology that allows vehicles to communicate with one another and share information about road conditions, as well as share various types of warnings [9]. VANET communication is based on IEEE standard known as Wireless in Vehicular Environment (WAVE). WAVE is the result of the development of 802.11, specifically 802.11p, which allocate 75 MHz bandwidth in the 5.9 GHz frequency spectrum for V2V and V2I communication. At 5.9 GHz, the 75 MHz spectrum is split into 7 channels, each with a 10 MHz bandwidth. Figure 1 depicts the 5.9 GHz frequency spectrum's channel segmentation. [2].

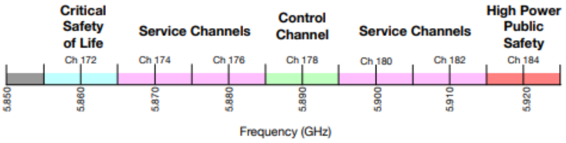

Fig. 1. Channels bandwidth allocation at 5.9 GHz frequency spectrum

In VANET, vehicles communicate with each other to share information needed for safety, comfort, and entertainment. The VANET communication architecture is divided into four categories [10]:

- In-vehicle communication: It is communication that aims to detect the condition of the vehicle and the driver
- Vehicle-to-vehicle: Communication between vehicles that is useful for sharing various kinds of information such as route information, various warnings, and information between drivers.
- Vehicle-to-infrastructure: It is communication that occurs between vehicles and the surrounding infrastructure such as the Road Side Unit (RSU). RSU on functions like a router that receives and sends information received from the vehicle and sends it to the intended destination. RSUs are allocated on the roadside with coverage distances depending on the equipment used.
- Vehicle-to-broadband communication: This means that communication on VANET vehicles can connect to other wireless network channels such as 3G and 4G because the cloud from the broadband can receive traffic information and monitoring data that can be useful for tracking vehicle location.

The VANET architecture is made up of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connectivity (V2I). The VANET system's supporting components are divided into two parts [11]:

- On-board Unit (OBU): OBU is a device in the vehicle to provide both V2V and V2I communication that placed on the vehicles.
- Roadside Unit (RSU): A network device that provide connectivity to various OBUs to the internet.

In order to secure communication in VANET, there are several parameters that need to be consider. The parameters that ensure this security are as follows [3]:

- Authentication: Ensure that the data entered by the user is correctly entered by the validated user, and that the data entered by the receiver is correctly entered by the sender.
- Availability: This is an important security parameter for VANETs since it is directly linked to the availability of security applications. VANET management must ensure the availability of services in the event of a problem or a malfunction.
- Confidentiality: Ensure that the message sent by the sender may only be accessed by the receiver.
- Integrity: Ensuring that the message sent by the sender does not change when it is received by the receiver.

UMN

B. Ad-hoc On-Demand Distance Vector

Ad-hoc On-demand Distance Vector (AODV) is commonly used routing protocol and a part of reactive routing protocols that work on-demand, which means that the protocol only establishes the path when it receive request from the node to engage in communication [12]. The AODV protocol utilizes two different mechanisms: route discovery and route maintenance. In discovering the route AODV broadcast a route request (RREQ) message to the neighboring node until it receives by the destination node. The destination or neighbor node that has a direct route to the destination receives RREQ, it will send a unicast route reply (RREP) message to the source node via a route where RREQ received (reverse route). The route to send the data will be chosen from the intermediate or destination node with a lowest hop count and a newest sequence number that is stored in the routing table. To notify if a route cannot be used, a Route Error message (RERR) is delivered and set the error route with invalid flag. If an invalid route is needed again, the route discovery process is repeated to find that route. The following are the fields stored on each AODV node [13]:

- Destination address: Contains the IP address of the destination node
- Sequence number: A number that continues to increase when an RREQ, RREP, and REER message is sent. The sequence number is used to determine the freshness of a route.
- Next hop: Store the address of the neighboring node.
- Hop count: The number of hops from the source node to the destination node.
- Lifetime: The time it takes for a node to receive the RREP message in milliseconds.

Routing flags: Showing the status of a route that shows valid if the route can still be used and shows invalid for routes that cannot be used.

C. Black Hole Attacks

Black hole attack is an attack carried out by pretending to be the shortest route to the destination which aims to get data and drop packets without continuing the message to the destination [14]. The black hole attack process is carried out by utilizing the route discovery process. When the source node sends an RREQ message, the attacker node pretends to have the shortest and newest route to the destination node by sending RREP packet with the lowest hop count and highest sequence number to the source node. This causes the source node to ignore RREP messages from other intermediate nodes and choose the route with the attacker node on it. Attacker node will drop the data that get through it, causing the data to never reach the destination node [6].

Figure 2 depicts AODV route discovery phase under black hole attack. As shown in the figure, the attack begins with the source node (S) broadcasting an RREQ message to the entire network in order to transfer data to the destination node (D). D which receives an RREQ from S then sends a RREP message with a hop count value of 2 and a sequence number of 125 through node I. When node M, a black hole node, gets an RREQ message, M sends an RREP message with the altered hop count and sequence number values of 1 and 4294967295. Because the AODV routing protocol takes the shortest delivery route indicated by the least hop count value and the latest route indicated by the greatest sequence number value, S who receives both RREP from D and M will choose the M route, which is a route that has black hole node on it, as a data transmission path [15].

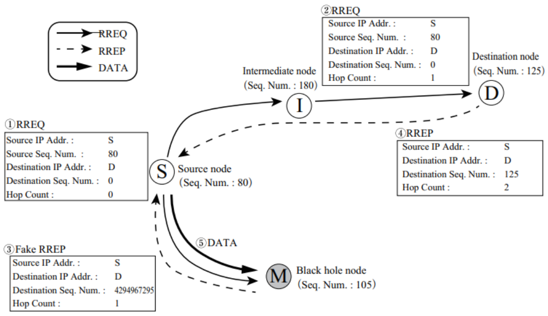

Fig. 2. Black hole attack in AODV

D. Modified Sequence Number

Modified Sequence Number (MSN) is a black hole attack detection method by utilizing the attack nature of the black hole that sends a RREP message with the highest sequence number (SN) value so that it is considered the latest path by the routing protocol. MSN detects black hole attack by establishing a threshold based on the maximum SN value of the RREP message that can be received by the source. If the RREP message received by the source has an SN value greater than the threshold, the source resends the RREQ message with the RREP sequence number as the retransmitted RREQ message's sequence number. When the source receives back an RREP message from the same node whose SN value is equal to the determined threshold value, the node is identified as a black hole attack, and the path from the message sent is not used to transmit data [8].

```
Src broadcast RREQ
Wait for RREP
On Receiving RREP
IF (RREP Sequence Number - SSN > TH)  {
    RRq by changing SSN to RREPSN
    Wait for RREP
    IF (RREPSN - SSN > TH)  {
    Black hole detected
    Discard the route
    }
}
Else {
    Send data using the route
}
```

Fig. 3. Pseudocode of MSN algorithm

The following is an explanation of the notation of the pseudocode in Fig.3 :

- Src: Source Node
- RRq: Re-broadcast RREQ
- SSN: Source sequence number
- RREPSN: Route reply sequence number
- TH: threshold

III. Methodology

Figure 4 illustrates the design that is the basis for the implementation of this research. The implementation begins by modifying the aodv.h and aodv.cc files by adding black hole attacks and MSN as black hole detection method. After modifying those files, black hole attack and added detection method are used in simulations in NS-2. The results of the simulation are in the form of a trace file and then processed using an AWK script that produces test metrics, namely detection rate (DR) and false alarm rate (FAR).

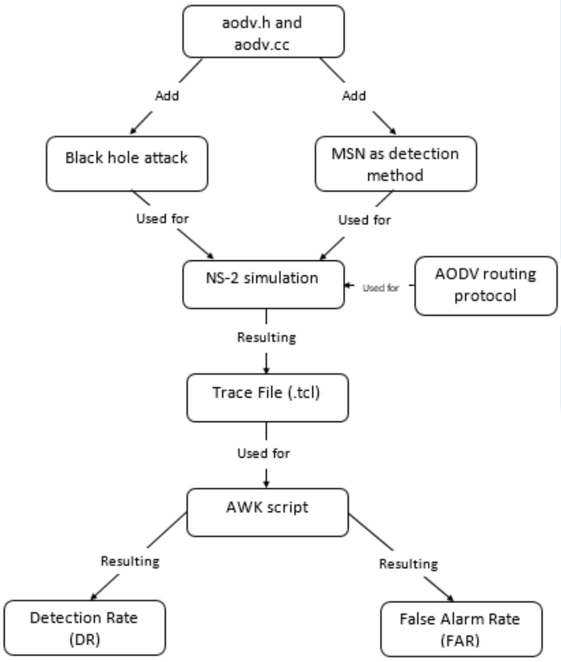

Fig. 4. Implementation Flow

To evaluate the performance of MSN algorithm, a sets of simulation were run on NS-2. The parameters of the simulations are detailed in Table 1.

TABLE I. Simulation Parameters

Parameter	Value
Simulator	Network Simulator 2 (ns-2.35), SUMO
Routing Protocol	AODV
Network Area	1000 m x 800 m
Packet Type	CBR
MAC	802.11p
Number of Nodes	20, 40, 50, 60, 80, 100
Attack Type	Black hole
Number of Attacker Nodes	1
Simulation Time	200 second
Packet Size	512 Kb
Number of CBR Packets Send	1, 5, 10, 15, 20
Mobility Model	Random way point

In the simulations, we chose one of the node as a black hole node, we assume that black hole nodes respond all RREQs with forged destination sequence number. The forged sequence number is the real sequence number from RREQ + 100 which is used as threshold.

To measure the performance of MSN algorithm in detecting black hole we use two different scenarios, node density and variations in number of CBR packets sent. The node density test was performed to determine the success of the MSN algorithm in identifying black hole attacks on VANET with varying vehicle counts [16]. Simulation of node density testing is performed on NS-2 with a total of one CBR package, one black hole node, and density variations of 20, 40, 60, 80, and 100 nodes. The scenario testing of the number of CBR packets was performed on NS-2 with a node density of 50 nodes, one black hole node, and changes in the number of CBR packets transmitted of 1, 5, 10, 15, and 20.s

The evaluation of MSN algorithm performance was done based on two parameters, Detection Rate (DR) and False Alarm Rate (FAR). DR is a method to measure the successfulness of MSN algorithm in detecting black hole attack. Equation (1) can be used to calculate the DR, whereas the FAR is a function used to measure the percentage error of a method in detecting attacks. The equation (2) can be used to calculate the FAR [7].

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP + FN}} \text{ X } 100\% \qquad (1)$$

With:

TP: Attacker node classified as attack.
FN: Normal node classified as attack.

$$\mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{TN + FP}} \text{ X } 100\% \qquad (2)$$

With:

FP: Attack node classified as normal.
TN: Normal node classified as normal.

IV. Results and Discussion

The first test to evaluate the detection performance of the MSN algorithm is to calculate the algorithm's DR value. Tests are run to determine the algorithm's success in detecting black hole attack on the network. The following are the findings of the MSN algorithm's DR testing against the two scenarios:

TABLE II. The results of DR tests on variations in the number of CBR packets

Number of CBR Packets Sent	True Positive (TP)	False Negative (FN)	Detection Rate (DR)%
1	38	17	69.0909
5	178	120	59.7315
10	457	321	58.7404
15	1188	1501	44.1800
20	2106	2738	43.4765

The results of the DR test on variations in the number of CBR packets with values of 1, 5, 10, 15, and 20 are shown in Table 2. The table of test results shows that the more CBR packets sent, the higher the TP and FN values, which influences the value of DR that determines the success of algorithm in detecting black hole attack. The results of the tests reveal that the MSN algorithm detection performance based on the DR parameter obtains the highest results in single CBR packet delivery, with the DR value reaching 69.0909% and dropping as the number of CBR packets grows, with the lowest value at 20 packets reaching 43.4765%.

TABLE III. The results of DR tests on variations in node density

Node Density	True Positive (TP)	False Negative (FN)	Detection Rate (DR)%
20	18	0	100
40	27	12	69.2038
60	17	10	62.9630
80	22	10	68.7500
100	30	0	100

Table 3 shows the results of the DR test on node density changes of 20, 40, 60, 80, and 100 nodes. The results shows that the MSN algorithm succeeded in detecting black hole attack at various node density situations, with DR values reaching 100% for densities of 20 and 100 nodes.

Another test to evaluate the performance of MSN algorithm is by testing it using FAR to calculate the detection error percentage in detecting black hole attack. The following are the results of the MSN algorithm's FAR testing against the two scenarios:

TABLE IV. The results of FAR tests on variations in the number of CBR packets.

Number of CBR Packets Sent	True Positive (TP)	False Negative (FN)	False Alarm Rate (FAR)%
1	0	37868	0.0000
5	0	141190	0.0000
10	0	341465	0.0000
15	2	721700	0.0003
20	47	1266549	0.0037

Table 4 shows the results of FAR testing on variations in the number of CBR packages with values of 1, 5, 10, 15, and 20. The results shows that the more CBR packages sent, the higher the TP and FN values, which influences the value of FAR. Table 5 shows that the MSN algorithm detection performance based on the FAR parameter is best when just one CBR packet is delivered at a time, and degrades as the number of CBR packets grows.

TABLE V. The results of DR tests on variations in node density.

Node Density	True Positive (TP)	False Negative (FN)	False Alarm Rate (FAR)%
20	0	9904	0,0000
40	0	22041	0,0000
60	0	30949	0,0000
80	0	47345	0,0000
100	0	67617	0,0000

Table 5 shows the results of the DR test on node density changes of 20, 40, 60, 80, and 100 nodes. The table of test results shows that the MSN algorithm detected black hole attacks in VANET at various node densities with a FAR value of 0.0000%.

V. Conclusion

To detect black hole attacks on VANET, this research implements the Modified Sequence Number (MSN) algorithm as a detection method. Based on results of the experiments, the MSN algorithm was successful in detecting black hole attacks on VANET. This success is shown by the detection rate (DR) test parameter value reaching 69.0909% when testing the number of CBR packets sent and 100% for testing the density of network nodes. The false alarm rate (FAR) test parameter is also used to determine the percentage of detection errors from the detection method. FAR testing results in the maximum percentage of detection errors, reaching 0.0037% when measuring the amount of CBR packets sent and 0% when testing network node density. From the research conducted, the success of the

UMN

MSN algorithm still does not take into account the effect of the characteristic parameters on the VANET on the DR and FAR test parameters, and does not take into account the detection method for the QoS of the VANET network. These two things can be the focus of further research.

REFERENCES

[1] A. Fitah, A. Badria, M. Moughit, and A. Sahel, “Performance of DSRC and WIFI for intelligent transport systems in VANET,” *Procedia Comput. Sci.*, vol. 127, pp. 360–368, 2018, doi: 10.1016/j.procs.2018.01.133.

[2] F. Arena, G. Pau, and A. Severino, “A review on IEEE 802.11p for intelligent transportation systems,” *J. Sens. Actuator Networks*, vol. 9, no. 2, pp. 1–11, 2020, doi: 10.3390/jsan9020022.

[3] J. Liang, M. S. Sheikh, and W. Wang, “A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs),” *Sensors (Switzerland)*, vol. 19, no. 16, 2019, doi: 10.3390/s19163589.

[4] Z. Afzal and M. Kumar, “Security of Vehicular Ad-Hoc Networks (VANET): A survey,” *J. Phys. Conf. Ser.*, vol. 1427, no. 1, 2020, doi: 10.1088/1742-6596/1427/1/012015.

[5] J. Grimaldo, *Performance comparison of routing protocols in VANETs under black hole attack in Panama City; Performance comparison of routing protocols in VANETs under black hole attack in Panama City*. 2018. doi: 10.1109/CONIELECOMP.2018.8327187.

[6] S. Lachdhaf, M. Mazouzi, and M. Abid, “Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol,” pp. 25–36, 2017, doi: 10.5121/csit.2017.71503.

[7] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, “Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET,” *Procedia Comput. Sci.*, vol. 151, pp. 1176–1181, 2019, doi: 10.1016/j.procs.2019.04.168.

[8] S. Shrestha, R. Baidya, B. Giri, and A. Thapa, “Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol,” *2020 8th Int. Electr. Eng. Congr. iEECON 2020*, pp. 2020–2023, 2020, doi: 10.1109/iEECON48109.2020.229555.

[9] H. F. Mahdi, M. S. Abood, and M. M. Hamdi, “Performance evaluation for vehicular ad-hoc networks based routing protocols,” *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 1080–1091, 2021, doi: 10.11591/EEI.V10I2.2943.

[10] T. Zaidi and S. Faisal, “An overview: Various attacks in VANET,” *2018 4th Int. Conf. Comput. Commun. Autom. ICCCA 2018*, no. July, pp. 1–6, 2018, doi: 10.1109/CCAA.2018.8777538.

[11] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Veh. Commun.*, vol. 7, no. January, pp. 7–20, 2017, doi: 10.1016/j.vehcom.2017.01.002.

[12] A. D. Devangavi and R. Gupta, “Routing protocols in VANET-A survey,” *Proc. 2017 Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2017*, pp. 163–167, May 2018, doi: 10.1109/SMARTTECHCON.2017.8358362.

[13] C. Perkins, E. Belding-Royer, and S. Das, “Network Working Group,” 2003.

[14] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, “A systematic review on security issues in vehicular ad hoc network,” *Secur. Priv.*, vol. 1, no. 5, p. e39, 2018, doi: 10.1002/spy2.39.

[15] T. Noguchi and M. Hayakawa, “Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks,” *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 539–544, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00082.

[16] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, “A reputation system for detection of black hole attack in vehicular networking,” *2015 Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. SSIC 2015 - Proc.*, no. August, 2015, doi: 10.1109/SSIC.2015.7245328.