Detecting Blackhole Attack using Encounter Records on Multi-Copy Routing Protocols in Delay Tolerant Networks (DTN)

Heru Nurwarsito, Naldo Steven Sirait

Abstract*: *Delay Tolerant Network (DTN) is a solution for intermittent connectivity and high delay. However, due to constrained connectivity, DTN is vulnerably susceptible to Blackhole attacks in which malicious nodes will drop all packets received from source nodes or relay nodes. The impact of a Blackhole attack can reduce the packet delivery ratio and waste resources from relay nodes that carry and forward messages. The encounter record scheme is one solution that can be applied to detect Blackhole attacks on the DTN. The encounter record mechanism is performed by utilizing a relay node that will store several records obtained from encounters between previous nodes, then the node will detect when a packet has dropped and a blacklist is performed on the node detected as a malicious node. Based on testing the performance of the routing protocol obtained that the encounter record scheme is able to detect malicious nodes so that it can again increase the delivery ratio and overhead ratio. The simulation results of this research showed that the Encounter Record has successfully detected Blackhole attacks with an average detection time of 1,5992 seconds in the spray-and-wait routing and 1,5342 seconds in the epidemic routing for 15 malicious nodes. Detection accuracy is 100% on spray-and-wait routing and 73,85% on routing epidemic for 15 malicious nodes.

Keywords*: *Blackhole Attack, Delay Tolerant Network, Encounter Record, Epidemic, Malicious nodes, Spray and Wait.

I. INTRODUCTION

Communication on the internet is based on packet switching. Packets are part of a complete block of user data (for example, part of an e-mail message or a page of a website) that travels from source to destination through a network of links connected by a router and two nodes exchanging data only when they are within the range of one transmission to another [1]. However, geographical conditions such as mountainous and coastal areas cause a lack of consistent connectivity. Delay Tolerant Network (DTN) was developed as a solution for a challenging network environment characterized by intermittent connectivity, long delays and frequent interruptions [2].

In a DTN network, a node can behave by dropping packets even though the node has enough buffers where this attack is included in a blackhole attack [1]. The Blackhole attack scheme is carried out by a malicious node that will drop all messages received despite having adequate buffer storage [2]. Blackhole attacks are divided into two types of attacks, namely single Blackhole attacks, and collaborative Blackhole attacks. Single Blackhole is a Blackhole attack carried out by one malicious node, while collaborative Blackhole is an attack carried out by more than one malicious node and attacks more relay nodes. The impact of a Blackhole attack will significantly reduce the performance of the delivery ratio and also waste resources from each relay node that has brought and forwarded the message being dropped.

The importance of detecting packet drop and reducing the impact of malicious nodes on DTN networks. Previous research [3] that used encounter record detection schemes in detecting flooding attacks on DTN networks. In this research, the encounter record can provide a high level of accuracy because of supporting information in determining the malicious node. Blackhole attacks can be detected using the Encounter Record detection scheme by utilizing the record generated when two nodes meet and exchange messages which will then store the results of the encounter record in buffers. A node will be considered dangerous if the resulting forwarding ratio is lower than a predetermined threshold [2]. Forwarding ratio is the ratio between the total number of messages sent by a node and the total number of messages dropped by that node. Where this scheme will function properly because the malicious node tends to drop the message it receives instead of sending it to the relay node or destination node.

Evaluating the performance of the routing protocol and scenarios in DTN requires an appropriate simulation tool in order to properly model the network. The Opportunistic Networking Environment (ONE) Simulator is a simulator that uses the Java language to provide a series of capabilities in simulating each DTN protocol within the ONE Simulator framework [4]. The need to evaluate the performance of each routing protocol that exists in DTN that has a delay in sending messages and the risk that messages are not sent on time or not at all. In this case, the performance parameters are message delivery probability, and latency average [4].

This research will apply a detection scheme to overcome the problem of malicious nodes that drop packets in the DTN network using the

Revised Manuscript Received on January 10, 2020.

Heru Nurwarsito, Lecturer of Computer Science Faculty, University of Brawijaya, Malang, East Java, Indonesia. Email: heru@ub.ac.id

Naldo Steven Sirait, Undergraduate Student of Computer Science Faculty, University of Brawijaya, Malang, East Java, Indonesia. Email: naldosteven@gmail.com

Retrieval Number: C10340193S20/2020©BEIESP
DOI: 10.35940/ijitee.C1034.0193S20

encounter record detection scheme. Successful use of the encounter record scheme will be known from the parameters of detection time and accuracy of the detection of Blackhole attacks.

This research will also compare the performance of each multi-copy routing protocol to determine the routing capabilities and the impact of each given test scenario. The results of the encounter record scheme provided in this research are expected to be able to detect attacks so as to improve routing performance again and be applied to various multi-copy routing protocols. Thus, there is no problem with packet drop on the DTN network so that it can be applied to real environmental conditions with limited network conditions. The encounter record scheme used will utilize the results of the records of each node so that it can detect the malicious node from the track record of each node meeting.

II. LITERATURE REVIEW

Blackhole attack is an attack carried out by a malicious node to be able to adapt to the network by getting the desired route, then the malicious node will drop all messages it receives despite having adequate buffer storage space [5]. Blackhole is a type of attack that has a significant impact on sending each message so that it will significantly reduce the performance of the delivery ratio and the waste resources that exist from each relay node that forwards messages from the node. In networks, nodes can move randomly (randomly deployed) or move selectively (selectively deployed) [1]. Malicious nodes have the same high connectivity as normal nodes, so they are often connected with other nodes. Based on research [2] if a normal node generates a packet to the destination node. On the other hand, the evil node does not produce its own packet. In this case, the malicious node will declare itself a normal relay node for all message destinations, but after the message is received, the malicious node drops the packet.

Several previous researches have detected Blackhole attacks [5] that use the Misbehavior Detection System (MDS) to detect and reduce the effects of bad nodes. The results show that when the packet drops, the high probability of MDS is able to achieve high detection rates and low false-positive rates for various scenarios in detecting dangerous nodes while maintaining low energy consumption for various DTN routing protocols [5]. The second research [1] used a distributed scheme to reduce the impact of attacks from the route of bad behavior and wrong node behavior. In the scheme a node will store several contact records obtained from the previous meeting, then the next node will detect whether a node has dropped a packet based on the contact record obtained [1]. Simulation results show that this scheme can effectively and efficiently detect and reduce the effects of the wrong route. The third research [2] used the Blackhole Detection and Grayhole attacker (SDBG) scheme to overcome black holes and Greyhole attacks carried out by one attack node or carried out by more than one attack node [2]. The simulation results show that SDBG can work well on various packages that may fall and the number of different evil nodes with high accuracy and fewer malicious node prediction errors.

In this research, using an Encounter record is one of the schemes for recording information traces when there are two nodes that meet and exchange messages, each node will generate an Encounter Record (ER) and store it in buffers. The meeting record itself includes the identities of the two nodes that contain the ER sequence number, the encounter timestamp, and the list of messages sent and received between the two nodes. The encounter record scheme is used in assessing malicious nodes by comparing forwarding ratios. Forwarding ratio is the ratio between the total number of messages received by a node from the source node or the relay node with the total number of messages that have been sent or forwarded [2]. In this case, the detection of malicious nodes is done when the two nodes make contact and send messages, then the two nodes exchange their meeting records that are stored in their respective buffers. Furthermore, the results of the record are used to determine the forwarding ratio metric that can distinguish between malicious nodes and normal nodes, and subsequently detected nodes will be blacklisted.

A. Blackhole Attack

Blackhole attacks are divided into two types of attack schemes, namely single Blackhole attacks, and collaborative Blackhole attacks. Single Blackhole is an attack carried out by a single malicious node, while collaborative Blackhole is an attack that has more than one malicious node on the network and attacks more relay nodes. The design of a Blackhole attack in this research was carried out using a malicious node that would drop packets so that the destination node would not receive messages. Malicious nodes used in black hole attack scenarios are 5 nodes and 10 nodes. When the source node sends a message, the malicious node that meets and receives a message from the relay node will then drop the message. The package drop process will continue until the predetermined simulation time [10].

Based on Figure 1 which shows the N1 and N2 nodes as normal nodes and M nodes as malicious nodes. The Blackhole attack scheme can be seen based on Fig. 1 carried out by node M as an individual malicious node. When node N1 will forward the message then meet node M, node N1 gives the message m1 and is stored in buffer node M. Furthermore, node N2 meets node M and passes the message m2 to node M. However, node M drops the message to the buffer node M where m1 and m2 packages are stored. Likewise, when node N3 encounters node M, packet drop will be carried out immediately after the message has entered the buffer node M as a malicious node [1].

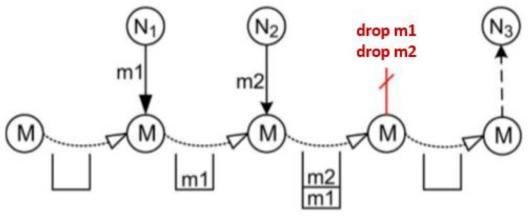

Fig. 1. Blackhole Attack Scheme

B. Encounter Record

Encounter record is one of the schemes for recording information traces when there are two nodes that meet and exchange messages, each node will produce an Encounter Record (ER) and then store it in buffers. The node is considered as a dangerous node if the forwarding ratio is lower than the predetermined threshold, while the higher forwarding ratio is estimated as a normal node [2].

This encounter scheme is able to function because a Blackhole attack will always drop the message it receives rather than forwarding the message. Based on Fig. 2 that shows nodes n1, n2 and n3 as normal nodes and m nodes as malicious nodes. When node n1 meets node m and forwards the message, node m will then drop the message it receives, but it will reduce the value of its forwarding ratio. And so on when node n2 exchanges messages with node m, node m will drop the message and reduce the forwarding ratio again. Finally, when node n3 exchanges messages with node m, node n3 evaluates the results of the ER record owned by node m. Where the forwarding ratio value is lower than the threshold, the node will be rated as a malicious node, which is then blacklisted.

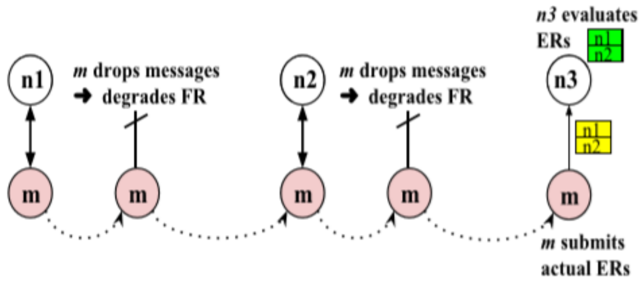

Fig. 2. Encounter Record Scheme

C. Performance Parameters

Performance parameters are test parameters used as a measure to compare the performance of each multi-copy routing protocol. The testing parameters used in this research are the delivery ratio and overhead ratio.

1) Delivery Ratio

The delivery ratio is the ratio of the number of packets sent from the source node and up to the destination node [5]. Testing on delivery ratio aims to test the success rate of one message that can be sent from source to destination, where the higher the value of the delivery ratio, the better the performance of the routing is given.

$$\text{Delivery Ratio} = \frac{\text{Total Delivered Message}}{\text{Total Created Message}} \times 100\% \qquad (1)$$

The formula used to get the delivery ratio results can be seen in (1). Based on (1) the total delivery message is the total number of messages sent successfully to the destination node and the total created message is the total number of messages sent. The results obtained through the parameters of the delivery ratio using units of a percent (%).

2) Overhead Ratio

Overhead Ratio is the number of replica messages that are forwarded to be able to send one message to reach the destination node [5]. Testing on the overhead ratio aims to test the performance of the routing protocol used, where the lower the value of the overhead ratio, the better the performance of the routing protocol used.

$$\text{Overhead Ratio} = \frac{\text{Relayed Message} - \text{Total Delivery Message}}{\text{Total Delivery Message}} \qquad (2)$$

The formula to get the overhead ratio results can be seen in (2). Based on (2), the relayed message is the number of messages that are relayed by the node and the total delivery message is the total number of messages successfully sent to the destination node.

III. SIMULATION SETTINGS

This section will explain each step in the design stage that will be carried out in this research. This design consists of two stages including simulation design and system configuration. The first stage will explain the design of simulations starting from the design of map and node mapping and scenario design. The second stage will be to configure the ONE Simulator application in accordance with the existing design.

A. Design of the Map Path

In the design of mapping, the node will move across locations in the Bangun Village and Karanggandu Village consisting of 50 nodes. The use of this area in this research is because it is a coastal area that has very low connectivity, so it is suitable for use in DTN networks. The movement model on the node used on this rural route is the Shortest Path Map-Based-Movement (SPMBM). The use of SPMBM is very suitable to be applied in this research because each node in its movement will follow the existing random path points of the map and then will determine the shortest routing to the node's point [6]. The average velocity of the moving node is simulated between 0.5 to 1.5 km/hr. Maps of the areas of the village of Bangun to Karanggandu are shown in Fig. 3.

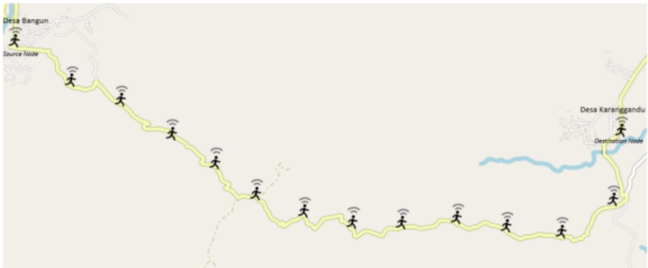

Fig. 3. Node Location Layout Design

B. Simulation Scenario

In this research, there are three simulation scenarios, namely the first simulation during normal conditions with no Blackhole attack or using an encounter record, the second simulation when there is a Blackhole attack but no encounter record, and the third simulation there is a Blackhole attack and using an encounter record. In each scenario that has been determined using parameters that are fixed.

C. Simulation Parameters

This research will use simulation parameters that will be used in each test research scenario. The parameters in this research use the map path Bangun Village to Karanggandu Village, Trenggalek Regency. The routing protocol used is epidemic and spray-and-wait with the network interface used is Bluetooth. The simulation time is 43200 seconds with 50 nodes used. The speed of motion of the node is divided into two, namely, the moving node is 0.5-1.5 Km / Hour with Time-To-Live used of 360 minutes. The buffer size used is 15MB with a message size of 500 KB-1000 KB.

The mobility model used is the Shortest Path Map-Based Movement.

IV. RESULT AND DISCUSSION

The testing phase in this research uses several test scenarios starting from the normal DTN network condition, then there is a black hole attack until it is detected using encounter records on the DTN network. In each scenario will explain the results obtained from the tests conducted. Furthermore, an analysis is performed on each scenario results obtained based on test parameters. The test parameters used in testing are delivery ratio and overhead ratio. In each scenario, 5 experiments will be conducted using a simulator.

A. Detection Time

Based on Fig. 4 shows the average test results of the time needed for an encounter record to detect black hole attacks, it shows that the spray-and-wait protocol has a slightly longer detection time than the epidemic protocol. Based on these results, the time difference obtained in the routing epidemic is due to flooding-based mechanisms that will distribute messages to each node that is encountered continuously so that the time to receive and exchange reports encounter records is faster, but too much resource is wasted due to the mechanism flooding. This mechanism causes the detection process with an encounter record to be slightly faster than spray-and-wait. Furthermore, the spray-and-wait protocol is able to reduce transmission overhead so that maximum performance is obtained in connection with the delivery delay in each scenario. In this case, the detection of encounter records has been done quickly because of better message distribution.

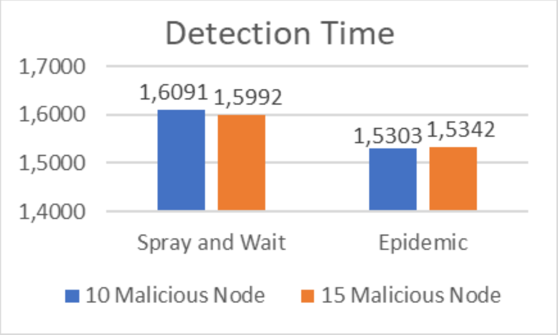

Fig. 4. Graphic Mean Detection Time

B. Detection Accuracy

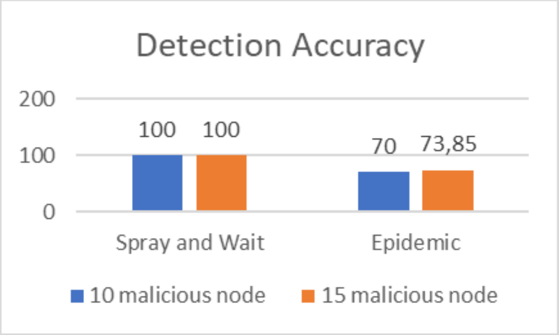

Fig. 5. Graphic Mean Detection Accuracy

Based on Fig. 5 shows the average test results show the accuracy has decreased in the routing epidemic when an additional malicious node occurs. Adding a malicious node causes the encounter record to misclassify the normal node into a malicious node. The process of dropping packets in the epidemic causes the Encounter Record to experience errors in comparing the number of replicas and treating normal nodes as malicious nodes. Epidemic routing protocols only send as many replicas as they can without a reduction in the number of replicas. So that the Encounter Record encountered an error in detecting the malicious node. In spray-and-wait routing, the addition of malicious nodes has no effect on detection accuracy. The detection process in the spray-and-wait routing is simpler because it only compares the number of replicas sent by the sending node to the number of replicas that the sender received. So the system can detect malicious nodes more accurately. This is due to the fact that despite the addition of a malicious node, the test results for both routings shows an accuracy value above 70%.

C. Delivery Ratio

Delivery ratio testing is to test the success rate of one message that can be sent from source to destination, where the higher the value of the delivery ratio, the better the routing performance obtained. The delivery ratio formula is obtained from (1). Based on Figure 6 shows the results of the delivery ratio performance in the first scenario with normal network conditions. Based on the average delivery ratio graph shown in Fig. 6, the spray-and-wait protocol averaged 51.01% and the epidemic protocol averaged 46.57%.

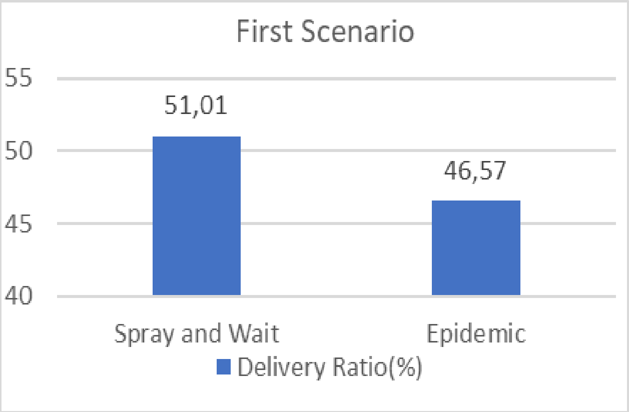

Fig. 6. Graphic of Average Delivery Ratio in the First Scenario

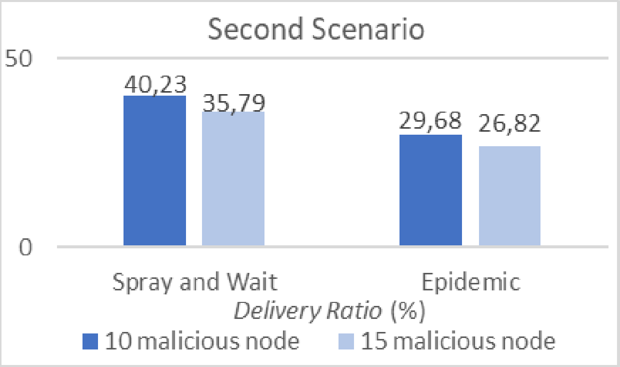

Fig. 7. Graphic of Average Delivery Ratio in the Second Scenario

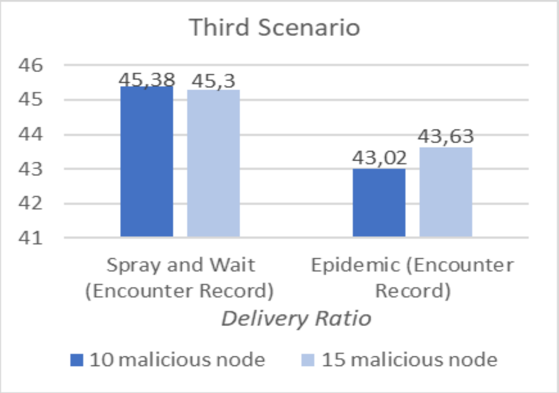

Fig. 8. Graphic of Average Delivery Ratio in the Third Scenario

Based on the simulation scenarios two scenarios are used to show differences in the performance of the routing protocol before and after the use of encounter records in black hole attacks. Based on Fig. 7 and Fig. 8 show the comparison of performance, delivery ratios on the protocol before and after use, find records in a Blackhole attack. Based on the graph of the average delivery ratio performed by Fig. 7, the results of the average delivery ratio to decrease during black hole attacks, namely the spray-and-wait protocol of 40.23% for 10 malicious nodes and 35.79% for the testing scheme 15 malicious node. Whereas the epidemic protocol is 29.68% for the 10 malicious node testing scheme and 26.82% for the 15 malicious nodes. The record meeting scheme that is applied to the number of bad nodes can still improve the average delivery ratio better then blacklist the nodes. Based on a graph of the average delivery ratio involving Fig. 8, the average delivery ratio increases again when meetings are applied to the spray-and-wait protocol by 45.38% for 10 dangerous nodes and 45.3% for the application of testing 15 malicious nodes. While the epidemic protocol is 43.02% for the 10 malicious node testing scheme and 43.63% for the 15 malicious nodes.

D. Overhead Ratio

This overhead ratio test is to provide a number of replicas of messages that are forwarded to be able to send one message to get to its destination. The overhead ratio formula is obtained from (2). Based on Fig. 9 shows the results of the overhead ratio performance in the first scenario with normal network conditions. Based on the graph of the average overhead ratio shown in Fig. 9, the spray-and-wait protocol averaged 4.6598 and the epidemic protocol averaged 137.2971.

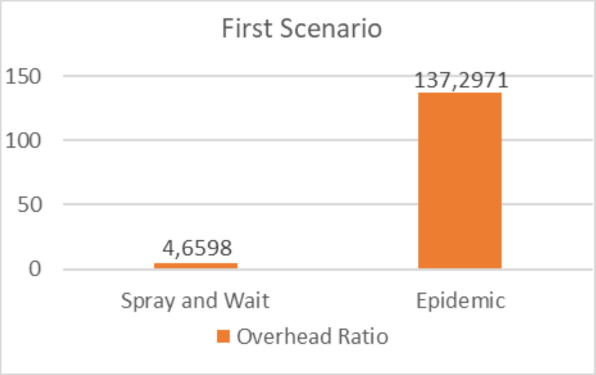

Fig. 9. Graphic of Average Overhead Ratio in the First Scenario

Based on the simulation scenarios, two scenarios are used to show differences in the performance of the routing protocol before and after the use of encounter records in black hole attacks. Based on Fig. 10 and Fig. 11 shows the comparison of overhead ratio performance on the protocol before and after the meeting found records in a Blackhole attack. Based on the graph of the average overhead cost ratio which shows Fig. 10 results of the ratio of the average cost of increasing the ratio of increase to the ratio of overhead costs, namely the spray-and-wait protocol of 7.3956 and 8.0663 for the 15 malicious node testing scheme. Whereas the epidemic protocol is 205,5449 for testing 10 malicious nodes and 229,4323 for 15 malicious nodes. From the results of tests carried out using meeting records resulted in an increase in the cost ratio of return by increasing the value of the additional cost ratio for both routing protocols. Change the meeting record in changing malicious nodes that stop the process of dropping messages, so the impact of dropping messages is reduced. Based on the average graph of overhead ratios involving Fig. 11, the average result of overhead ratios that were increased again when the encounter was applied to the spray-and-wait protocol was 4.7986 for 10 malicious nodes and 5.4724 for the application of 15 malicious nodes. node While the epidemic protocol is 204.8393 for testing 10 malicious node schemes and 206,5002 on 15 malicious nodes.

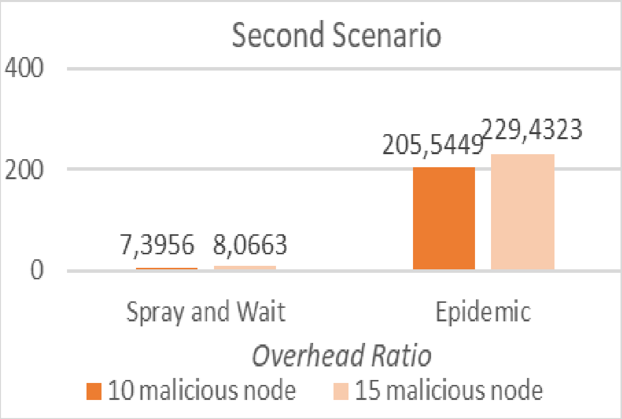

Fig. 10. Graphic of Average Overhead Ratio in the Second Scenario

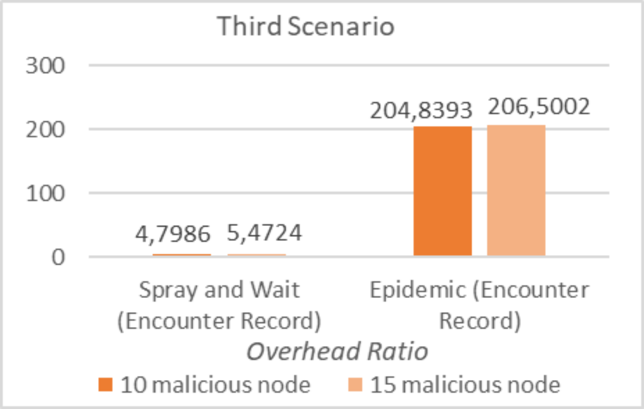

Fig. 11. Graphic of Average Overhead Ratio in the Third Scenario

V. CONCLUSION

Based on the use of encounter record schemes that have been carried out by utilizing packet records from relay nodes that contain traces of encounters from each node on the network, the average time of an encounter record detects a Blackhole attack of 1.6091 seconds at 10 malicious nodes and 1.5992 seconds at 15 malicious nodes for spray-and-wait, while the average detection time is 1.5303 seconds for 10 malicious nodes and 1.5342 seconds for 15 malicious nodes in epidemics. On the other hand, the average accuracy of using encounter records is 100% for all spray-and-wait attack schemes, while the average accuracy is 70% on 10 malicious nodes and 73.85% on 15 malicious nodes for epidemics.

The performance of multi-copy routing protocols based on the delivery ratio parameter has decreased performance when there is a Blackhole attack from normal network conditions, with an average of 40.23% in spray-and-wait and 29.68% in epidemics for 10 malicious nodes, then 35.79% in spray-and-wait and 26.82% in epidemics for 15 malicious nodes. On the other hand detection of encounter record is able to overcome black hole attacks so that the average delivery ratio increases again, which is 45.38% for spray-and-wait and 43.02% for epidemics for 10 malicious nodes, then 45.3% for spray -and-wait and 43.63% in the epidemic for 15 malicious nodes. Furthermore, the overhead ratio parameter also decreases performance when there is a Blackhole attack with an increase in the overhead ratio, which is an average of 7.3956 on spray-and-wait and 205.5449 on epidemic for 10 malicious nodes, then 8.0663 on spray- and-wait and 229,4323 in the epidemic for 15 malicious nodes. On the other hand, detection of encounter record is able to overcome black hole attacks so that the average overhead ratio decreases again, namely by an average of 4.7986 in spray-and-wait and 205.8393 in epidemics for 10 malicious nodes, then 5.4724 in spray-and-wait and 206,5002 epidemics for 15 malicious nodes.

REFERENCES

1. Q. Li and G. Cao, “Mitigating routing misbehavior in disruption tolerant networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 664–675, 2012.
2. T. N. D. Pham and C. K. Yeo, “Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks,” *IEEE Trans. Mob. Comput.*, vol. 15, no. 5, pp. 1116–1129, 2016.
3. P. T. N. Diep and C. K. Yeo, “Detecting flooding attack in delay tolerant networks by piggybacking encounter records,” *2015 IEEE 2nd Int. Conf. information science Secure. ICISS 2015*, pp. 1–4, 2016.
4. A. Keränen, J. Ott, and T. Kärkkäinen, “The ONE simulator for DTN protocol evaluation,” *SIMUTools 2009 - 2nd Int. ICST Conf. Simul. Tools Tech.*, 2009.
5. M. I. Ratu, B. Soelistijanto, M. T. Informatika, and J. Afandi, “Analisis kinerja routing protokol spray and wait di jaringan opportunistic,” pp. 69–79.
6. N. Mehta and M. Shah, “Performance of Efficient Routing Protocol in Delay Tolerant Network: A Comparative Survey,” *Int. J. Futur. Gener. Commun. Netw.*, vol. 7, no. 1, pp. 151–158, 2014.
7. F. Warthman, “Delay-Tolerant Networks (DTNs): A Tutorial v1.1,” vol. 39, no. 3, 2012.
8. A. Vahdat and D. Becker, “Epidemic Routing for Partially-Connected Ad Hoc Networks. Technical Report CS-200006. Department of Computer Science, Duke University. Recuperado de: http://issg.cs.duke.edu/epidemic/epidemic.pdf,” 2000.
9. T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and wait: An efficient routing scheme for intermittently connected mobile networks,” *Proc. ACM SIGCOMM 2005 Work. Delay-Tolerant Networking, WDTN 2005*, pp. 252–259, 2005.
10. Y. Guo, S. Schildt, and L. Wolf, “Detecting blackhole and Greyhole attacks in vehicular Delay Tolerant Networks,” *2013 5th Int. Conf. Commun. Syst. Networks, COMSNETS 2013*, 2013.
11. F. Li, J. Wu, and A. Srinivasan, “Thwarting Blackhole attacks in disruption-tolerant networks using encounter tickets,” *Proc. - IEEE INFOCOM*, pp. 2428–2436, 2009.

AUTHORS PROFILE

Heru Nurwarsito, was graduated from Electrical Engineering Universitas Brawijaya in 1989 and continued at Informatics Engineering in the Institute of Technology Sepuluh Nopember for the Magister Program. He was a lecturer in the Department of Electrical Engineering Universitas Brawijaya from 1987 until 2009, then a lecturer in the Department of Informatics Engineering Universitas Brawijaya from 2010 until Now.
His research area focuses on computer networking, Software engineering, the Internet of Things and Applied of Smart Technology.

Naldo Steven Sirait, was undergraduate Student of Computer Science Faculty, University of Brawijaya, Malang, East Java, Indonesia.
His research area focuses on computer networking and the Internet of Things

.