International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209985 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

Red-AODV: A Prevention Model of Black Hole Attack for VANET Protocols and Identification of Malicious Nodes in VANET

Md. Tofael Ahmed
Department of Information and Communication Technology, Comilla University, Bangladesh
tofael@cou.ac.bd

Amina Aktar Rubi
Department of Information and Communication Technology, Comilla University, Bangladesh
rubi1309026@gmail.com

Md. Saifur Rahman
Department of Information and Communication Technology, Comilla University, Bangladesh
saifurice@cou.ac.bd

Maqsudur Rahman
Department of Computer Science and Engineering, Port City International University, Bangladesh
mrrajon.ict04@gmail.com

Received: 29 July 2021 / Revised: 02 September 2021 / Accepted: 25 September 2021 / Published: 27 October 2021

Abstract – VANET is a type of MANET in which the Vehicle nodes communicate between each other using wireless medium without any fixed infrastructure. The major goal of VANET is to create a safer and more efficient Intelligent Transportation System (ITS) and Traffic Information System (TIS) where high-mobility drivers may communicate with one another. Routing protocols, we know, accomplish the shortest possible connection time while using the least amount of network resources. VANETs also have some routing protocols to implement it in the real world for proper communication among vehicles. The Black Hole Attack has become one of the security dangers in VANET because of the great mobility of the vehicles and the volatile nature of the network connections. As the name imply, the Black Hole Attack in VANET is similar to the Black Hole in the universe which makes entities disappeared. Black Hole Attack redirects the data packets to such a node that actually does not exist in the network. In this research, we analyzed the performances of one reactive protocol (AODV) and one proactive protocol (OLSR) in order to better categorize the protocol's robustness under Black Hole Attack and approach a prevention model, named Red-AODV to keep VANET safe from Black Hole Attack. After applying the Red-AODV protocol in the network which may reduce the losses resulted from the existence of Black Hole Attack, then again we analyze the changings of the network performance. We use Network Simulator 2 and run it for different number of nodes. The simulations are made in terms of several network parameters including Packet Delivery Ratio (PDR), Dropped Packet Ratio (DPR) and End to End Delay (EED), Throughput and Normalized Routing Load (NRL).

Index Terms – VANET, Black Hole Attack, AODV, Red-AODV, Intelligent Transport System.

1. INTRODUCTION

VANET is one of the most special kinds of MANET where Intelligent Transport System (ITS) is used for communication which includes the vehicles as well as road side infrastructure [1]. In VANET, the communication functions like packet forwarding, route table management, error detection, multipath detection, shortest path selection are done by the routing protocols. In the VANET, there are numerous routing protocols. AODV, AOMDV, DSDV, DSR, OLSR, GPSR, TORA etc. are some of the examples.

In VANET, communication among the high speedy nodes is done in a short range as quickly as possible. So there are some challenges for VANET to be considered in this situation like reliability, confidentiality, consistency and efficiency, probability of the interference, the security of the communication. Now the big question is what is the obstacle to ensure security? The answer is the existence of various types of attacks in VANET. BHA, or Black Hole Attack, is a noteworthy attack.

RESEARCH ARTICLE

The malicious node presents itself as having the least lengthy path and secretly drops packets flowing through it in a black-hole attack [2]. If we can detect the untrusted node then it will be possible to avoid them at the time of communication. The identification of malicious nodes can be divided into two types: prevention-based and detection-based. Encryption and authentication are widely used as the prevention based techniques. The detection based techniques contain again two types, signature based and anomaly based, where the former finds out the attacked profiles with suspicious kind of behavior and the latter discovers the abnormalities from pre-established normal profile. In the anomaly based malicious node detection we see that the malicious node is detected by comparing the performance parameters of both situations. So this technique will be employed in the detection technique.

This research is conducted to present a detection technique for malicious nodes of VANEL protocols such as AODV and OLSR with comprehensive performance analysis. And also in this research, a prevention model name Red-AODV is presented which prevents the Black Hole attach with considerable accuracy.

In this research, we developed a comprehensive framework describing the key features of Network Simulator 2 (NS2) in designing VANET containing multiple malicious nodes. We generated malicious nodes and evaluated their behavior in the black hole attack situation. The performance of reactive and proactive protocols were also evaluated for better categorization of the protocols robustness under malicious conditions and then we also analyzed the change in performance after applying our proposed protocol. We used three different network loads to analyze the parameters in both malicious and non-malicious scenario. Finally we proposed an advanced version of one of the VANET (Red-AODV) protocols that can detect and avoid a node which is attacked by the Black Hole Attack by not sending the data packet through that node.

NS2 is used here as the simulator and the proposed Red-AODV scheme is compared to the fundamental AODV routing protocol, this results are examined on various network performance metrics.

Our contribution of this work are as following:

- We identified the presence of Black Hole Attack in VANET protocols i.e. AODV and OLSR.
- We proposed a new model named Red-AODV which prevents the Black Hole Attack with considerable accuracy.

2. RELATED WORKS

Black Hole Attack detection has become an important area of research. When a node is under any kind of attack, it may exhibit many types of misbehaviors like packet dropping, packet modification, delay, jamming etc. called malicious behavior. By measuring the differences among various parameters we can detect the malicious nodes. Some authors have studied both traffic measurement and anomaly detection techniques for detecting malicious nodes. And some other authors have proposed many solutions on this regard. There has been some researches proposed for detecting and preventing Black Hole Attack for MANETs. These researches can be used to implement the same task in VANET. In this section, some types of researches related to our work are discussed.

Patel et al. [3] proposed to detect the malicious nodes by the anomaly detection technique and in addition, presented an improved AODV protocol to avoid such malicious nodes when a route is established in MANET. To draw the conclusion they compared the result of the parameters-throughput and route discovery time in both scenarios (malicious and reliable) to detect the malicious nodes. They only used two parameters but in our study, we used more parameters like PDR, DPR and EED and also compared the results among all protocols.

Jain et al. [4] used trust-based AODV protocol to measure the performance during the black hole attack. To detect and change the effect of the black hole assault, they used Gauss Markov mobility and Random walk mobility to examine the packet delivery ratio and throughput. In their work, they presented prevention for only AODV protocol but in our research, we presented prevention model for three protocols and we also presented a method to identify the malicious nodes with five performance parameters. Ananthi et al. [5] have worked with four different attacks and sinkhole attack and draw a conclusion that the black hole attack occurs if the data transmission is blocked by any intermediate nodes. They have used two parameters to detect the attacks and then they compared the results. In our research we got better throughput than theirs and our end to end delay is also very much less than theirs. We also presented three more additional performance parameters and compared all the parameters in our research.

Kumar et al. [6] used entropy to detect numerous malicious nodes and devised a malicious node packet identification algorithm to lower the effect of dos attack (MMPDA). In their work, Multiple hostile nodes are detected using bandwidth and threshold values, whereas irrelevant nodes are found using entropy. Their work only presents the detection of malicious nodes, but in out work we presented the detection of malicious nodes as well as a prevention model. Sathish et al. [7] have detected and prevented the single and collaborative black hole attacks by broadcasting a fake RREQ with non-existing destination address. As the destination does not exist, any node responding to the source by sending an

RESEARCH ARTICLE

RREP is detected as malicious node and put in black hole list. The author proposed a digital signature and a trust value method to prevent the black hole impact. This work also lacks the inclusion of a prevention model which we have addressed in our research. Khatoun et al. [8] proposed a reputation system where they used a watch dog to check if any modification in the received packet's information is made or not and to identify the black hole attack. They also calculate a reputation score which detected the nodes that dropped frequently of the packets. Here the calculation depended on the reports sent by its neighbors. This is why the proposed model fails in the presence of cooperative black hole attacks which is limitation of their work.

Jahan et al. [9] presented a double acknowledgement packet routing strategy for detecting and preventing nodes that are malicious. In the strategy, every intermediate node has to send an ACK message so that the source node can be informed that it has forwarded the packet to the next node and when the packet reaches the destination, the process of sending acknowledgement ends. Due to sending the ACK this routing strategy causes extra delay which is a setback of their research.

Hiremath et al. [10] detected and prevented the Black Hole attack with an adaptive system using fuzzy interference. For picking the next hop neighbor to forward data, the Fuzzy Interference System (FIS) is used. The architects of FIS employed four inputs to characterize the quality of the next hop neighborhood: data, trust, data rate, data loss, and energy, which are provided periodically by each node to update neighbor information. The paper contained the simulation result of proposed model showing a better performance. Their research only presents a detection system but in our research, we have added a prevention model with extensive performance analysis. The model proposed by Kumar et al. [11] is compared to an adaptive method, where in the simulation results the new proposed model shows a better performance. Their work shows different detection techniques but lacks the presentation of prevention models.

Deshmukh et al. [12] proposed a secured AODV protocol to detect and prevent single and cooperative black hole attacks. A validity value to the RREP is attached without changing the basic mechanism of AODV. The simulation results comparing to the fundamental AODV shows a good performance against the Black Hole attack. However the proposed method falls flat, when an intelligent adaptive black hole node can claim that it has the shortest route by setting the validity value in the same way.

In [13], K.C. Purohit et al. presented a solution for mitigation of black hole attack in VANET. They presented the performance of the malicious nodes using five performance metrics. Their works lacks the inclusion of a prevention model which we have addressed in our research. An approach based on the detection and response strategy has been presented by B. Sun et al. in [14]. In their work, the black hole attack is spotted during the detection phase using a next-hop approach. If the attackers collaborate to create the false reply packets, this scheme will fail which is a drawback of their research.

To combat cooperative black hole attacks, Tamilselvan et al. suggested PCBHA based approach on the AODV protocol in [15]. Furthermore, several solutions based on intrusion detection or reputation scores are also presented in their work. But they only presented their work for 25 nodes. In our research we worked with three different node values (30, 60, 90). S. Kurosawa et al. in [16] also presented a detection system for black hole attack using dynamic learning method. They only simulated their model for 30 node value and their work also lacks the inclusion of a prevention model which we have addressed in our research.

In addition to the limitations of current research, in this work, we have proposed a prevention model for detecting Black Hole Attack with extensive research which we have discussed in the further sections.

3. PROPOSED RED-AODV MODEL

3.1. Design Methodology of the Proposed Model

When an AODV protocol source node wants to deliver a data packet to a given destination node, it first examines its routing database to see if the path exists. If such is the case, the data is sent down that conduit. If no suitable path can be identified in the routing table, the source node uses the route discovery procedure to find a new path to the destination.

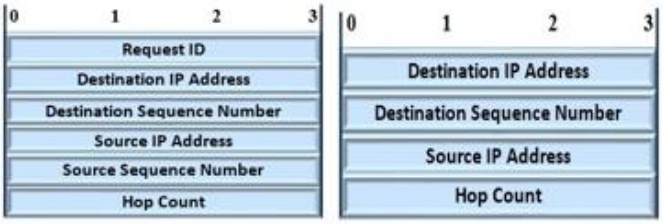

Figure 1 RREQ (Left) and RREP (Right) Packet Format of AODV

Figure 2 RREQ (Left) and RREP (Right) Packet Format of Red-AODV

The source node initiates the route discovery phase by broadcasting a Route Request packet. A neighbor node sends

RESEARCH ARTICLE

a Route Reply packet (RREP) to the source if it has a valid route to the target node or if the neighbor node is the desired destination. As illustrated in Figure 1, we make a minor alteration to the main functional mechanism in the AODV protocol's route discovery process in our suggested model (Red-AODV).

In Red-AODV, we encrypt the destination address by using a hash function, e.g. Cyclic Redundancy Check 32 bits (CRC-32) [17]. Comparing Figure 1 with Figure 2, we see that the only change is made on the RREQ packet format, where the source node encrypts the destination address in RREQ packet with the CRC-32 value of the destination. Note that the destination address and the CRC-32 value of the destination value both have a length of 32bits [18] and that is the reason of the RREQ format being the same and will not cause any extra overhead in the protocol.

3.2. Workflow Diagram of the Proposed Model

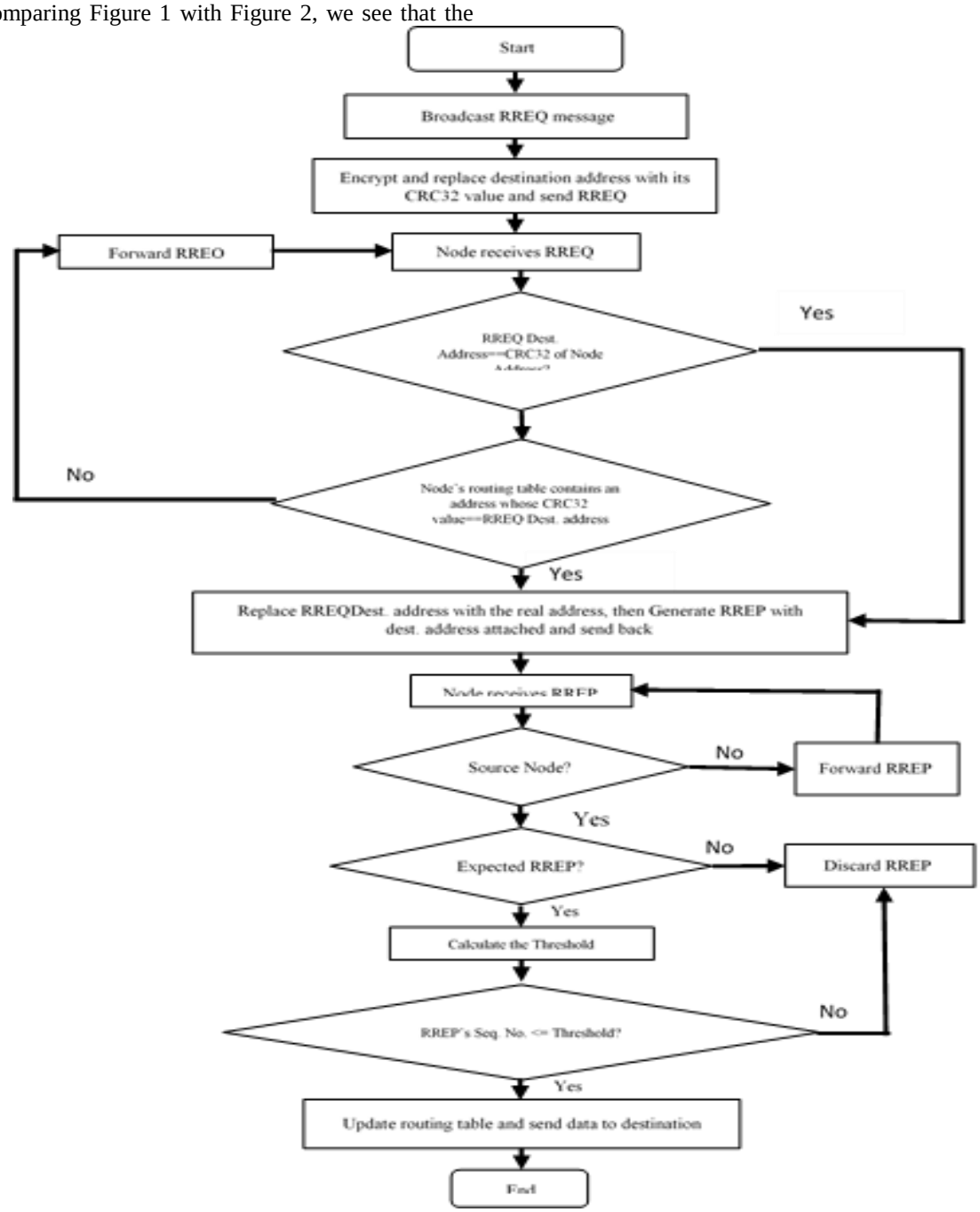

Figure 3 Flowchart of RED-AODV

RESEARCH ARTICLE

In Red-AODV, when a source node desire to initiate data transmission, first of all it stores the real destination address for its own and sends a RREQ packet to all of its neighbor nodes, where the destination address is replaced with its CRC-32 value in RREQ. If a neighbor node that receive the RREQ packet is the destination itself or it has a shortest route, then the neighbor node replies to the source node by placing the real address in the RREP packet. There are two conditions. The intermediate neighbor node does this by calculating the CRC-32 value of its own IP address (if the node is the intended destination), and then comparing that with the one set in the RREQ packet.

Or calculating the CRC-32 value of each route available in intermediate neighbor's routing table (if the node is not the intended destination) and then comparing that with the one set in the RREQ packet.

If both the conditions are false, then the intermediate node just forwards the RREQ packet to the next node. The source node may receive a many RREPs from different intermediate nodes. All the RREPs must go through two phases of checking mechanism:

If RREP's destination address is unexpected (not the destination address stored by source), source will discard the RREP. Because, only the attacker nodes send RREP with destination address that does not exist.

RREP holds a valid destination address, then its sequence number is compared to a threshold.

If sequence number < = threshold; then the RREP is accepted and routing table is updated.

Or, if sequence number > threshold; then the RREP is discarded.

Suppose, the source node receives 'n' number of RREP packets, then it calculates the threshold value as follows:

$$\text{Threshold} = \frac{\text{1st RREPs' seq. no.+ 2nd RREPs' seq. no.+. . . .+nth RREPs' seq. no.}}{n} + \text{MINIMUM (1st RREPs' seq. no, 2nd RREPs' seq. no, ... , nth RREPs' seq. no)}$$

The Red-AODV protocol will prevent the black hole attack in the first phase of the checking mechanism. But in case of adaptive black hole, it is tough to detect and prevent because the attacker node just act like a valid node. It also maintains a routing table and checks it for the intended destination node address. If the attacker node finds a destination address in its routing table that can be accepted by the source node as the freshest route, it sends a RREP with the destination address having high sequence number. No matter, our proposed model (Red-AODV) can prevent such kind of adaptive black hole node in the second phase.

Our proposed model (Red-AODV) is able to detect and prevent Black Hole Attacks. Since it is not possible to reverse CRC-32, so a group of black hole node cannot get the real destination address. Hence, Red-AODV will reject any unexpected RREP with an invalid destination address.

4. RESULTS AND DISCUSSION

4.1. Simulation Environment

4.1.1. Simulation Modeling

Simulation is the first step of any application for analyzing the performance and the service quality before implementing in the real world. For our detection we used the following factors:

- The traffic model: we use NSG topology design software to create the network and the TCL file.
- Antenna Model: the omnidirectional antenna has been used in our work for transmitting and receiving the packets
- Communication model: we employed 802.11g as the mac layer for the characteristics of radio used by node with proper frequency.
- Traffic model: the TCP CBR is used in the node for sending traffic to destination.
- Wireless signal propagation: two ray ground reflection propagation model has been implemented.

4.1.2. Simulation Tools

The tools used in the simulation are given below:

- Hardware: RAM: 4GB, Processor: Core i3
- Operating System: Ubuntu 18.04 LTS, Windows 7, 64bit
- Network Design Tool: NSG version 2.1
- Simulator: Network Simulator 2.35 (NS2)
- Performance Analyzer: AWK (Aho Weignberger Kernighan) Programming Language

4.1.3. Network Simulator 2.35 (NS2)

A network simulator calculates the interaction among the network entities named router, switch, access point, node etc. one of the best open source simulator for networking is known as network simulator version 2 shortly NS2 [19]. NS2 provides the support to implement several network protocols in wired and wireless network for simulating various performance parameters.

Two programming language: C++ and OTcL are used in ns2. OTcl creates the simulation by assembling and configuring the components, while C++ describes the simulator's internal mechanism. The linkage between the two languages is done

RESEARCH ARTICLE

by TclCL [20]. The network simulator works with the network's TCL file. The command 'ns' creates two files: a Network Animator file (NAM) and a Trace file, the NAM file displaying network animation and the trace file containing network information such as created packets, send packets, protocol utilized, and so on.

4.1.4. Simulation Methodology

Various protocols are used in VANET. When the nodes communicate with one another sometime they behave like a malicious node. These malicious behavior are called security attack. In this work we tried to find out the behaviors of the VANET node when they are good and malicious.

There are few steps to complete the work. They are Protocol Implementation, Black hole Declaration, Network Design, Malicious Node Declaration, NS2 Implementation, Performance Analysis and Graphical Representation4

4.1.5. Protocol Implementation

In this paper we deal with three protocols named AODV, AOMDV and OLSR. In NS-2.35 there are some build in protocols. AODV and AOMDV are two of them. The OLSR protocol is not implemented in the simulator. So to work with this protocol we have implemented this in the NS-2.35 folder. Then we run the command 'make' in the command prompt to complete the task.

4.1.6. Black Hole Declaration

As we have to deal with good and malicious nodes, there should be some prescribed way of finding out which node is good and which one is malicious. There are various ways to perform the task. In our work, we use the concept of black hole attack. The function of the black hole attack is dropping the packets it receives. By the following procedures we can declare the function of a black hole attacker in ns2 which acts as a malicious node.

Declare a variable name attacker in the protocol.h file Initialize the attacker variable as false in the protocol.cc file. That means the node will act as a trusted node. Now if a node is a malicious the variable attacker becomes true. If the node is attacker then its function is dropping the packets it receives. This function is added in the protocol.cc file. By these procedure we have declared the function of a black hole attacker which is a malicious node.

4.1.7. Network design

In our research, we have worked with different network load. The network consisted of Node 30 (Low network load), Node 60 (Medium network load), Node 90 (High network load).

The main network was designed by the NSG tool. In this tool there are different options to design a wired and wireless network. As VANET is a wireless network so we used the wireless network design. By the waypoint option the movement of the nodes are given. We used the TCP protocol to transmit a packet from the source to destination which works with the ftp protocol. There are various parameters to simulate the VANET network. The chart of the parameters are shown in Table 1.

Parameter Name	Initialization
Channel Type	Wireless channel
Propagation Model	Two Ray Ground Reflection
Mac Protocol Type	MAC 802.11
Queue Type	Drop Tail/Priority Queue
Link Layer Type	Link Layer
Antenna Type	Omnidirectional
Max Packet in Queue	50
Routing Protocol	AODV, OLSR and Red-AODV
Mobility Model	Random Waypoint
Nodes Type	Mobile Node
Connection Type	CBR, TCP

Table 1 Parameter Initialization for Wireless Network (VANET)

The last option of this tool is creating the TCL (Tool Command Language) file. This is the network file we designed for the VANET network. And the network simulator works with this file to generate the output.

4.1.8. Malicious Node Declaration

From the previous section we crated the TCL file for a network. Thus we have created 3 TCL file for the network load 30, 60 and 90 respectively. The TCL files created for each protocol. Until now, all the node act as trusted nodes. Now the second part of the work is declaring some malicious node using the black hole attack. From the black hole attack declaration section we see that when a node becomes an attacker node then it starts to drop the packets it receives. So the new TCL files that contains the attacker nodes must show some different behavior than the previous network.

The declaration of malicious node in ns2 is done in the TCL file using the following statement.

$ns at 1.0 "[$n35 set ragent_] Blackhole"

From the code we see that when the simulation time is 1ms, the node number 35 (may be another node) holds the value black hole. So the attacker variable declared in the *.cc file

RESEARCH ARTICLE

becomes true and the node acts as a malicious node and it starts the activity of dropping the packets it receives.

4.1.9. NS2 Implementation

This is the core part of the implementation section. We have two types of TCL files for the protocols in different network load. One types of TCL file contains no malicious node where another types contains few defected node which are declared as black hole attacker. The NS2 simulator runs the TCL file and creates two additional files i.e. Network Animator (NAM) file and Trace file. The NAM file is the graphical representation of the network we designed through TCL file. This animator file shows the packet delivery from source to destination. Another file created by the NS2 simulator is the trace file which contains all the information of the network like send packets, protocol used, agents and other information. The following fig shows a trace file image.

4.1.10. Performance Analysis and Graphical Representation

This is the final part of the simulation to find out the performance parameters of the network for different load in the both scenario. The sceneries are normal and malicious network. To find out three performance parameters: PDR, DPR, EED, Throughput and NRL. We create an AWK script. Then each of the trace file is analyzed by the AWK script to find out the performance of each network using the protocols separately. We use the same networks of three different sizes for each protocol in both situation. So all other factors like node distance, node communication range, interference range etc. are same. This analysis shows only text values. To make the result more attractive we used the Microsoft excel tool to represent the result graphically.

4.2. Performance Metrics

To analyze the network characteristics we have to evaluate few parameters. There are a lots of parameters and we choose three of them as below:

- Packet Delivery Ratio (PDR)
- Dropped Packet Ratio (DPR)
- End-to-End Delay (EED)
- Throughput
- Normalized Routing Load (NRL)

4.2.1. Packet Delivery Ratio (PDR)

Packet delivery ratio indicates one of the most important quality of service of a network. It's the proportion of total packets received at the destination by the CBR sink to total packets originated by the CBR source [21].

$$\text{PDR} = \frac{Number\ of\ packet\ received}{Number\ of\ packet\ sent} \quad (1)$$

A higher ratio of the PDR indicates a better performance of the network. So if the PDR increases, the QoS also gets improved with it. The PDR and Malicious PDR all protocols are analyzed separately in different network load (30, 60, 90 nodes). Then the performance are compared in the both scenario. Table 2 shows the PDR and malicious PDR scores among protocols. From Table 2, we see that the PDR of AODV is much better in all networks. But in any kind of network we can see that the PDR is reduced when the protocol contains few malicious node. So the malicious node decreases the PDR in AODV protocol.

Protocols	Node	Sent Packet	Received Packet	PDR (%)
AODV	30	355	289	81.40
	60	357	317	88.79
	90	372	135	78.48
Malicious AODV	30	95	64	67.36
	60	50	37	74
	90	33	22	66.66
OSLR	30	621	268	43.15
	60	1622	202	12.45
	90	1345	203	15.09
Malicious OSLR	30	625	252	40.32
	60	1589	178	11.20
	90	1122	137	12.21
Red-AODV	30	355	286	80.6
	60	357	310	86.8
	90	172	131	76.10
Malicious Red-AODV	30	98	78	79.59
	60	50	42	84
	90	33	26	78.78

Table 2 PDR and Malicious PDR among Protocols

RESEARCH ARTICLE

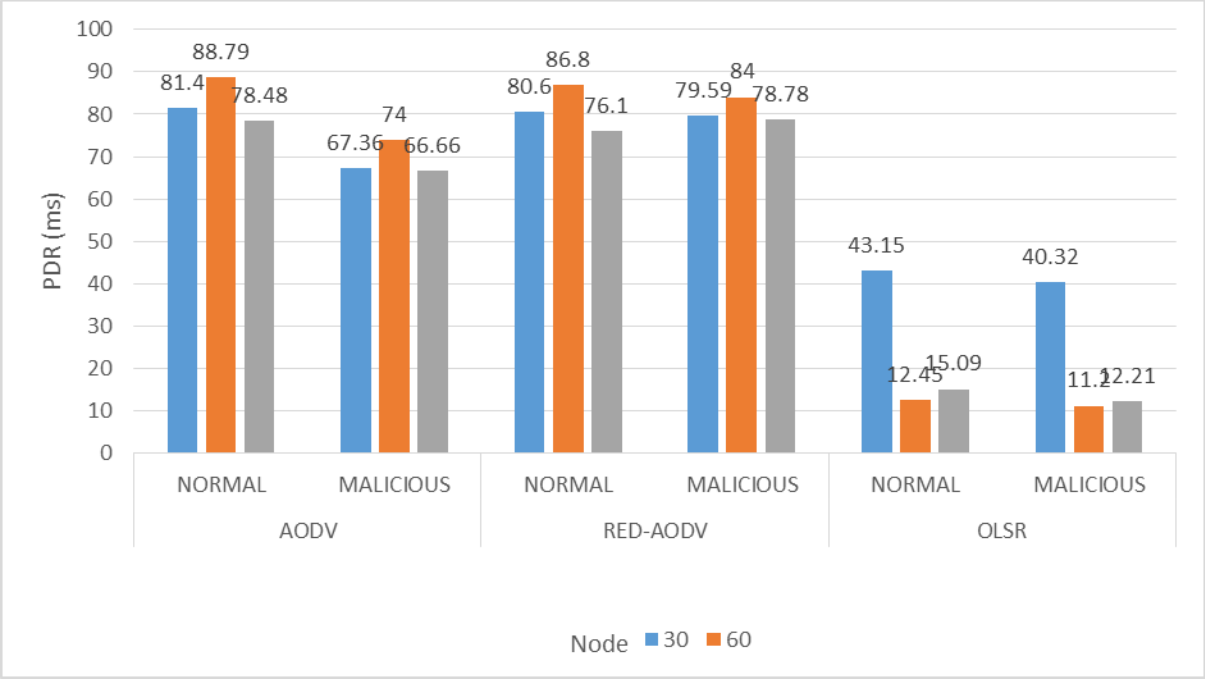

Figure 4 Comparison of PDR Value of Trusted and Malicious Red-AODV with Other Protocols

In the same network where the AODV networks performs well, the OLSR protocol performs a low PDR in the both case of trusted and malicious nodes. But our focus is on the PDR of both scenario to detect the malicious node. From the analysis we can say that the PDR is decreased in the malicious situation. So this helps to find out the difference between normal and malicious state. PDR of Red-AODV is much better and almost same as AODV in all networks. We also see that despite of having few malicious node the PDR of Red-AODV is not decreased that much as like as AODV. So the malicious node cannot decreases the PDR in Red-AODV protocol in that level. Figure 4 shows a comparison of PDR and malicious PDR for our three routing protocol. The PDR performance isn't our main concern. Our main focus is on the difference between the PDR in the normal and anomalous conditions and to see whether our newly developed protocol performs well in the presence of few malicious nodes. From Figure 4 we can see that the PDR for any network and for any protocol is reduced in the malicious situation compared with the normal one, but for Red-AODV it does not work that much. So we can say that the malicious nodes reduce the Packet Delivery Ratio of a network AOVD, OLSR, but not Red-AODV.

4.2.2. Dropped Packet Ratio (DPR)

The Dropped Packet Ratio is the number of lost packets divided by the total number of packets sent. When a node becomes an attacker node then it starts to drop packet [22].

$$DPR = \frac{Number\ of\ packet\ lost}{Number\ of\ packet\ sent} \quad (2)$$

Each packet has a deadline by which it must be executed. The scheduler attempts to reduce the amount of packets lost due to deadline expiration if the deadline is not reached. DPR indicates the bad performance of the network. Increasing the DPR means degrading the quality. Table 3 shows the DPR and malicious DPR scores among protocols.

Table 3 shows that in case of Dropped packet ratio the AODV protocol is showing a better performance in the large network load. The smaller the DPR the better the performance. Now looking into the table we can see that the DPR is higher in the malicious condition which means the malicious nodes degrade network performances. The difference in the DPR is the main point to look at. So the malicious node changes the normal performance in AODV. DPR is much smaller in the OLSR protocol in the both situations when the network is loaded with malicious node or trusted node. To find out the malicious node we have to focus on the individual performance of the network. Though the DPR is small in both the situation but comparing with each other the DPR is higher in the malicious situation than the normal one. So the malicious nodes have affected the network performance. In case of Dropped packet ratio, Red-AODV protocol shows a better performance than AODV. Looking into table 3, we can see that in the malicious condition the DPR is a little bit higher, which is negligible comparing with the original AODV protocol. So we can say that Red-AODV drops less packets in the presence of malicious nodes compared to AODV. Figure 5 shows a comparison of DPR and malicious DPR for our three routing protocol.

RESEARCH ARTICLE

Protocols	Node	Sent Packet	Dropped Packet	DPR (%)
AODV	30	355	95	26.76
	60	357	47	13.16
	90	172	32	18.60
Malicious AODV	30	95	42	44.21
	60	50	14	28
	90	33	10	30.30
OLSR	30	621	23	3.70
	60	1622	46	2.83
	90	1345	147	10.92
Malicious OLSR	30	625	39	6.24
	60	1589	42	2.64
	90	1122	219	19.51
Red-AODV	30	355	87	24.50
	60	357	41	11.48
	90	172	28	16.28
Malicious Red-AODV	30	95	29	30.5
	60	50	9	16.18
	90	33	7	21.21

Table 3 DPR and Malicious DPR among Protocols

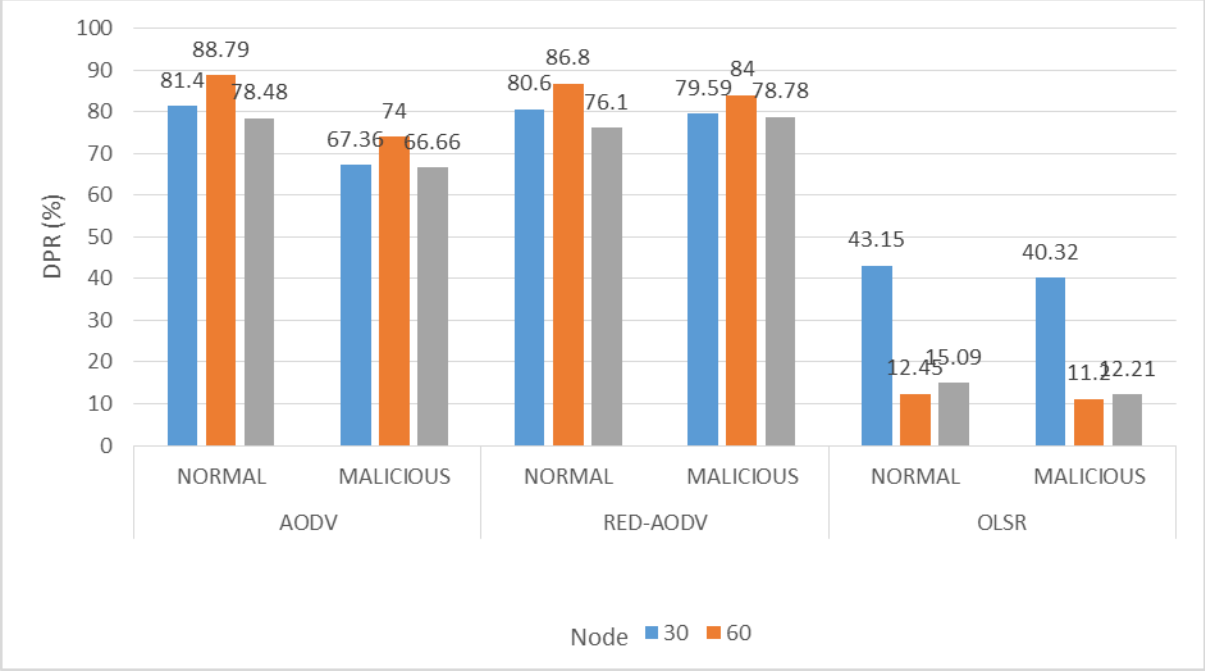

Figure 5 Comparison of DPR Value of Trusted and Malicious Red-AODV with other Protocols

From the figure 5, we can see that the DPR is higher in the malicious protocol than the normal one in any kind of network load except the middle-size network of the OLSR protocol. We assume that this is an exceptional event. Ignoring this exception we can say the malicious node degrades the performance of the network by increasing the Dropped Packet Ratio. Also Red-AODV is performing well by not dropping packets inspite of having some malicious node.

4.2.3. End-to-End Delay (EED)

The time it takes for a packet to travel from its source to its destination, including its processing time, is known as end-to-end delay. Most of the time EED is calculated from the sum

RESEARCH ARTICLE

of Process Delay (PD), Queuing Time (QT), Transmission Time (TT) and Propagation Time (PT)].

$$EED = PD + QT + TT + PT \quad (3)$$

When the network take the small EED that means the network is working perfectly. But in the big network the EED may be higher naturally. Table 4 shows the EED and malicious EED scores among protocols.

From the output shown in Table 4, we see that the EED of the trusted AODV and the malicious AODV is much different. As few nodes are malicious so different path have to be set up and for this reason it takes more time to deliver the packets. In this case low network load will take less time to deliver the packets as the congestion is low here. The malicious node increase the EED of the network in the AODV protocol. The OLSR protocol shows the reverse results from other protocols. It takes less time when the network is more heavily loaded. Comparing the both situation of malicious and normal the EED is higher in the malicious conditions. The increasing of the EED means the decreasing of the network performance.

EED of the trusted Red-AODV and the malicious Red-AODV is much similar. As few nodes are malicious, but as Red-AODV has technique to detect malicious node, so it does not have to interact with those nodes which causes less time to deliver the packets. In the case of low network load, e.g. when there are 30 nodes, the congestion is low. So it will take less time to deliver the packets.

In the case of heavy network load, e.g. when there are 90 nodes, the congestion is also high. So it will take some more time to deliver the packets. Figure 6 shows a comparison of EED and malicious EED for our three routing protocol. From Figure 6, it indicates that the EED is much higher in the anomalous network where the malicious nodes are present. In case of EED, OLSR shows much better performance comparing AODV and Red-AODV. This is because OLSR is a proactive or table driven protocol. Hence the sending node has the path available in advance to reach the destination. That is why OLSR consumes less time for each transmission.

Node	AODV (ms)	Malicious AODV (ms)	OLSR (ms)	Malicious OLSR (ms)	Red-AODV (ms)	Malicious Red-AODV (ms)
30	76.71	88.2	34.39	41.76	57.21	63.33
60	106.58	238.15	14.16	14.14	112.67	131.51
90	94.84	185.43	12.6	13.41	84.18	112.43

Table 4 DPR and Malicious DPR among Protocols

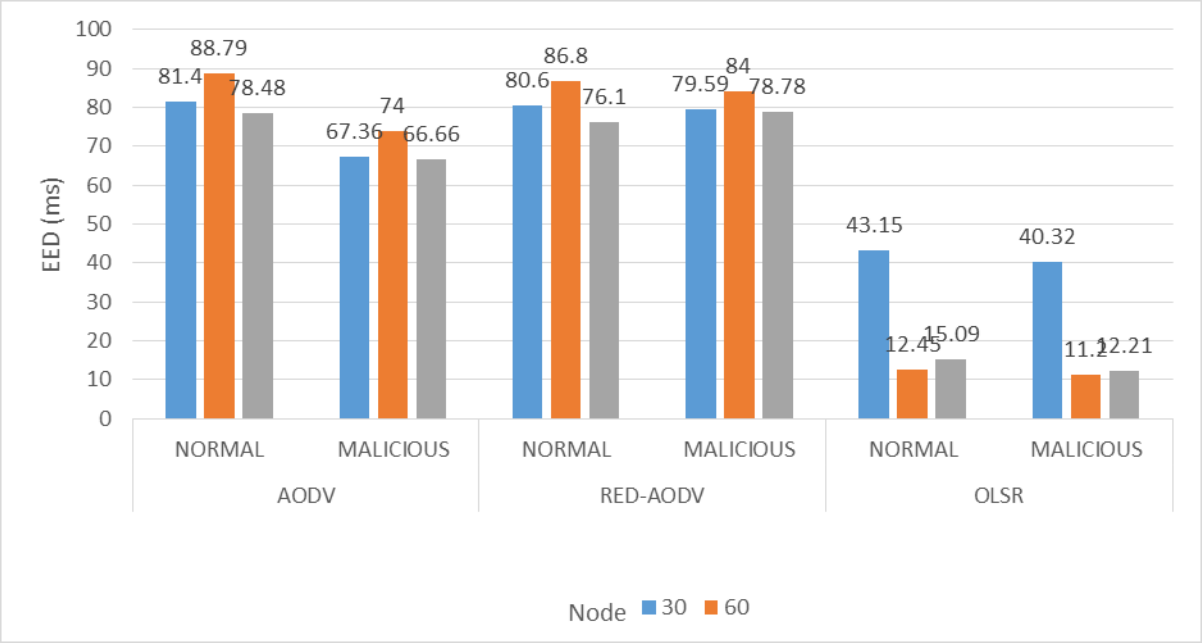

Figure 6 Comparison of EED Value of Trusted and Malicious Red-AODV with other Protocols

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209985 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

4.2.4. Throughput

In digital networking, throughput is an important term which refers to the amount of data (actually the number of bits) transferred between source and destination within a given time frame. In short, throughput measures how many packets reach at the destination successfully. Throughput is measured in Bits Per Second (bps).

$$\text{Throughput} = \frac{Number\ of\ packet\ received * bits\ per\ packet}{Given\ Time\ Frame} \quad (4)$$

Table 5 shows the throughput and malicious throughput scores among protocols.

From table 5, it can be seen that the throughput values of trusted AODV is much better than Malicious AODV for all three nodes. As throughput refers to how much data can be transferred from source to destination within a given timeframe, we can say that AODV trusted AODV protocol will transfer much more data within the given timeframe than the Malicious AODV protocol. In case of OLSR, the difference between OLSR and Malicious OLSR is also notable and the trusted OLSR also has better throughput value than the Malicious OLSR protocol for all three nodes. And finally, the difference of throughput value of trusted Red-AODV and Malicious Red-AODV is also notable from the table which indicates that Red-AODV is also performing considerably well.

Figure 7 shows a comparison of throughput and malicious throughput for our three routing protocol.

From figure 7, it is evident that the throughput value of trusted Red-AODV is much higher than the malicious Red-AODV. In case of throughput, Red-AODV is performing far better than AODV protocol though its performance is little less than OLSR.

Node	AODV	Malicious AODV	OLSR	Malicious OLSR	Red-AODV	Malicious Red-AODV
30	30.33	17.83	101.83	83	81.33	69
60	51.16	38	143	110.33	116.83	110
90	82	61.83	172	138.16	142	128.16

Table 5 Throughput and Malicious Throughput among Protocols

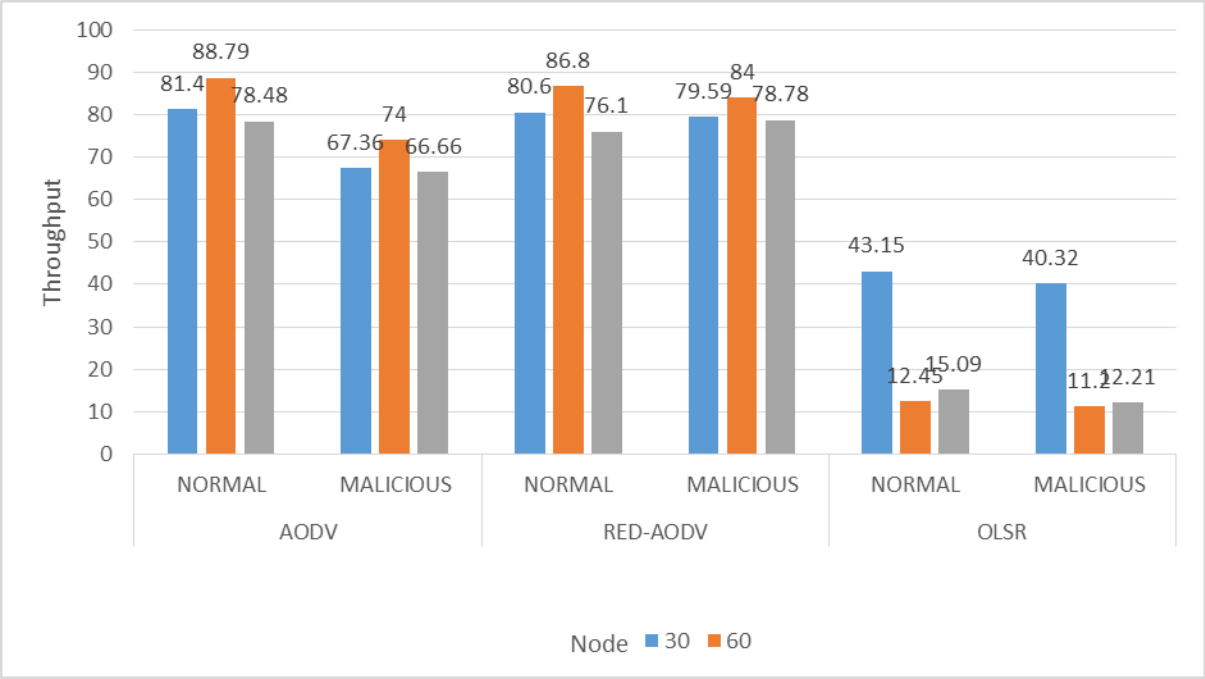

Figure 7 Comparison of Throughput Value of Trusted and Malicious Red-AODV with other Protocols

RESEARCH ARTICLE

4.2.5. Normalized Routing Load (NRL)

NLR is the amount of data that a particular number of nodes (not all nodes) in a specific network are ready to send at a specific time. A standard network is that which is designed with a capacity which will be more than enough to handle the network routing load at any time. The network capacity should be more than adequate to handle the traffic load, which is a basic goal for most network architectures. Whether a proposed model is having adequate capacity to handle any network load is the biggest challenge nowadays. NRL is also measured in bits per second (bps).

Table 6 shows the NRL and malicious NRL scores among protocols.

Table 6 shows that the NRL values of all the protocols are gradually increasing as the number of nodes grows. In case of OLSR and Malicious OLSR, the difference in NRL value is quite noticeable. But in case of AODV and Malicious AODV, there is a little difference in NRL value which differentiates the trusted nodes from the malicious nodes. Furthermore, for Red-AODV the difference between the NRL values are also notable.

Figure 8 shows a comparison of NRL and malicious NRL for our three routing protocol. From figure 8, we can again clearly see that for NRL, the trusted Red-AODV protocol values are better than malicious Red-AODV. Also in case of NRL, Red-AODV is showing much greater performance than AODV.

Node	AODV	Malicious AODV	OLSR	Malicious OLSR	Red-AODV	Malicious Red-AODV
30	18.67	16.33	54.16	36.83	36.5	33
60	20.17	17	81.5	58.16	51.83	46.33
90	23.83	18.66	97.16	72	70.67	63.67

Table 6 NRL and Malicious NRL among Protocols

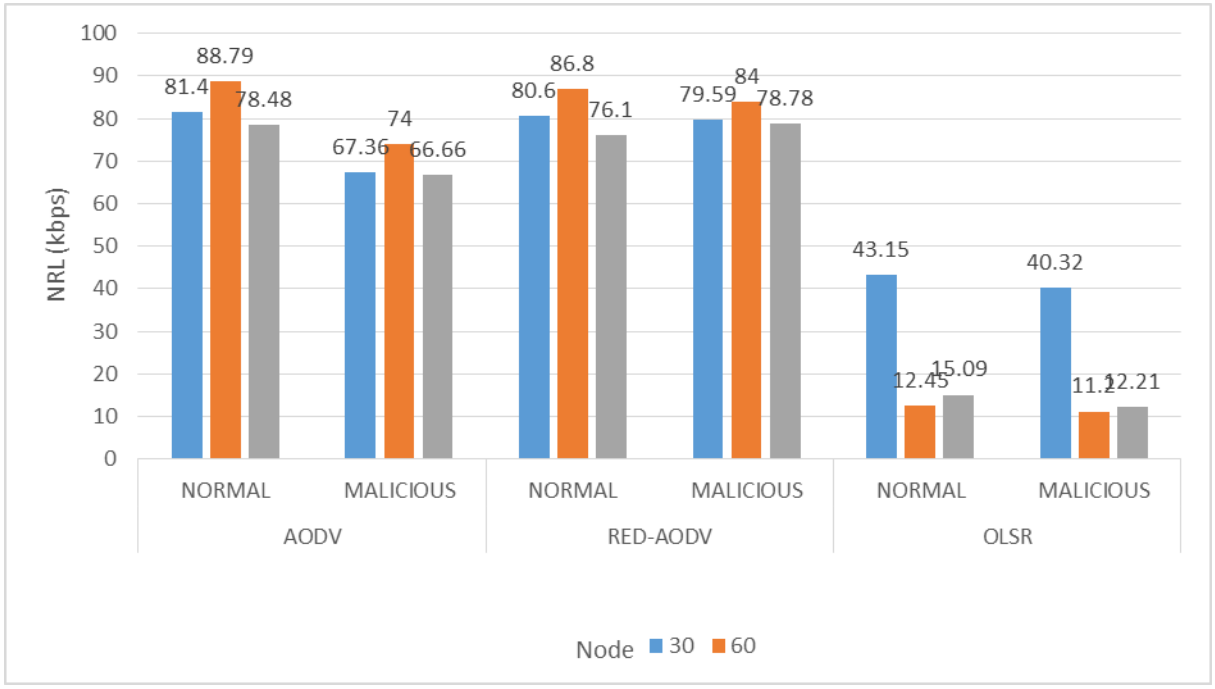

Figure 8 Comparison of NRL Value of Trusted and Malicious Red-AODV with other Protocols

5. CONCLUSION AND FUTURE WORK

The main purpose of this work is to show how to model a VANET containing malicious nodes using NS2 and to detect the malicious nodes by applying anomaly detection technique, and also design an advanced AOVD (Red-AODV) protocol that is able to perform better than AODV in the presence of malicious node. In our work, first we have developed the Red-AODV protocol, then we have compared the performance of this new Red-AODV protocol with two other routing protocols: AODV and OLSR with different network sizes (30,

RESEARCH ARTICLE

60 and 90). The process of the anomaly detection is based on comparing various performance parameters in the normal and malicious scenarios. We developed Red-AODV by using a hash function that is we have encrypted the destination address by attaching CRC32 bits, so that the black hole nodes get confused to guess the real destination address. After developing the Red-AODV protocol, we have evaluated its performance. We have used three performance parameters: Packet Delivery Ratio (PDR), Dropped Packet Ratio (DPR), End to End Delay (EED), Throughput and Normalized Routing Load (NRL) to evaluate the performance to detect the presence of the malicious nodes. This is done in two steps. In the first step, we evaluate the three parameters for the normal protocols for different network sizes. Then we create an environment for the black hole attack in the protocols and through the TCL file by declaring few nodes as black-hole attacker that have made the protocols defected. Finally we evaluate the performance parameters for the same networks for the infected protocols. . Our future work will be on developing an advanced proactive protocol (advanced OLSR) by using the same hash function that is, encrypting the destination address by attaching CRC32 bits, so that OLSR protocol can perform better in the presence of black hole node.

REFERENCES

[1] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[2] R. Mishra, A. Singh, and R. Kumar, "Vanet security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016, pp. 1050–1055.

[3] K. S. Patel and J. Shah, "Detection and avoidance of malicious node in manet," in *2015 International Conference on Computer, Communication and Control (IC4)*. IEEE, 2015, pp. 1–4.

[4] A. Jain, U. Prajapati, and P. Chouhan, "Trust based mechanism with aodv protocol for prevention of black-hole attack in manet scenario," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*. IEEE, 2016, pp. 1–4.

[5] J. V. Ananthi and S. Vengatesan, "Detection of various attacks in wireless adhoc networks and its performance analysis," in *2017 International Conference on Inventive Computing and Informatics (ICICI)*. IEEE, 2017, pp. 754–757.

[6] S. Kumar and K. S. Mann, "Detection of multiple malicious nodes using entropy for mitigating the effect of denial of service attack in vanets," in *2018 4th International conference on computing sciences (ICCS)*. IEEE, 2018, pp. 72–79.

[7] M. Sathish, K. Arumugam, S. N. Pari, and V. Harikrishnan, "Detection of single and collaborative black hole attack in manet," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2016, pp. 2040–2044.

[8] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, "A reputation system for detection of black hole attack in vehicular networking," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2015, pp. 1–5.

[9] R. Jahan and P. Suman, "Detection of malicious node and development of routing strategy in vanet," in *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2016, pp. 472–476.

[10] P. Hiremath, T. Anuradha, and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in manets," in *2016 International Conference on Information Science (ICIS)*. IEEE, 2016, pp. 245–251.

[11] A. Kumar, M. Bansal *et al.*, "A review on vanet security attacks and their countermeasure," in *2017 4th international conference on signal processing, computing and control (ISPCC)*. IEEE, 2017, pp. 580–585.

[12] S. R. Deshmukh, P. Chatur, and N. B. Bhople, "Aodv-based secure routing against blackhole attack in manet," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2016, pp. 1960–1964.

[13] K. C. Purohit, S. C. Dimri, and S. Jasola, "Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (VANET)," *Wirel. Pers. Commun.*, vol. 97, no. 4, pp. 5099–5114, 2017.

[14] B. Sun, "Detecting black-hole attack in mobile ad hoc networks," in *5th European Personal Mobile Communications Conference 2003*, 2003.

[15] L. Tamilselvan and D. V. Sankaranarayanan, "Prevention of Cooperative Black Hole Attack in MANET," *Journal of Networks*, vol. 3, no. 5, pp. 13–20, 2008.

[16] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," *Com.tw*. [Online]. Available: http://ijns.jalaxy.com.tw/contents/ijns-v5-n3/ijns-2007-v5-n3-p338-346.pdf. [Accessed: 16-Sep-2021].

[17] "Cyclic redundancy check (crc) rfc," https://tools.ietf.org/html/rfc3385.

[18] C. Perkins, E. Belding-Royer, S. Das *et al.*, "Ad hoc on-demand distance vector (aodv) routing," 2003.

[19] W. contributors, "Network simulation," https://cutt.ly/kmeEBfk, Jun 2021.

[20] "Network simulator 2 (ns2): Features & basic architecture of ns2," https://cutt.ly/1meEMw0.

[21] M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (wsns)," in *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*. IEEE, 2013, pp. 324–329.

[22] "Packet loss ratio," https://cutt.ly/tmeE4AJ.

Authors

Md. Tofael Ahmed is the Associate Professor of ICT, Comilla University (Bangladesh). Research area includes Cyberbulling Detection, Data Mining, Text Analytic, Big Data, Online Social Network analysis.

Amina Aktar Rubi received her B.Sc. and M.Sc. degrees in Information and Communication Technology from the Department of Information and Communication Technology, Comilla University, Bangladesh. Her research interests include Network Security, Comparative Performance Analysis.

Md Saifur Rahman got his B.Sc. (Honours) and M.Sc. degrees in Information and Communication Engineering from the University of Rajshahi in Rajshahi, Bangladesh In 2006 and 2007. In 2012, he began working as a Lecturer at Comilla University's Department of Information and Communication Technology in Comilla, Bangladesh, where he is now an Assistant Professor.

RESEARCH ARTICLE

Maqsudur Rahman is the Senior Lecturer at Department of Computer Science and Engineering, Port City International University, (Bangladesh). His teaching interests include Computer Programming, Computer Networks, Data Communication, and Mobile Communication, as well as Digital Communication, Internet of Things, and Network Security.

How to cite this article:

Md. Tofael Ahmed, Amina Aktar Rubi, Md. Saifur Rahman, Maqsudur Rahman, "Red-AODV: A Prevention Model of Black Hole Attack for VANET Protocols and Identification of Malicious Nodes in VANET", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 524-537, 2021, DOI: 10.22247/ijcna/2021/209985.